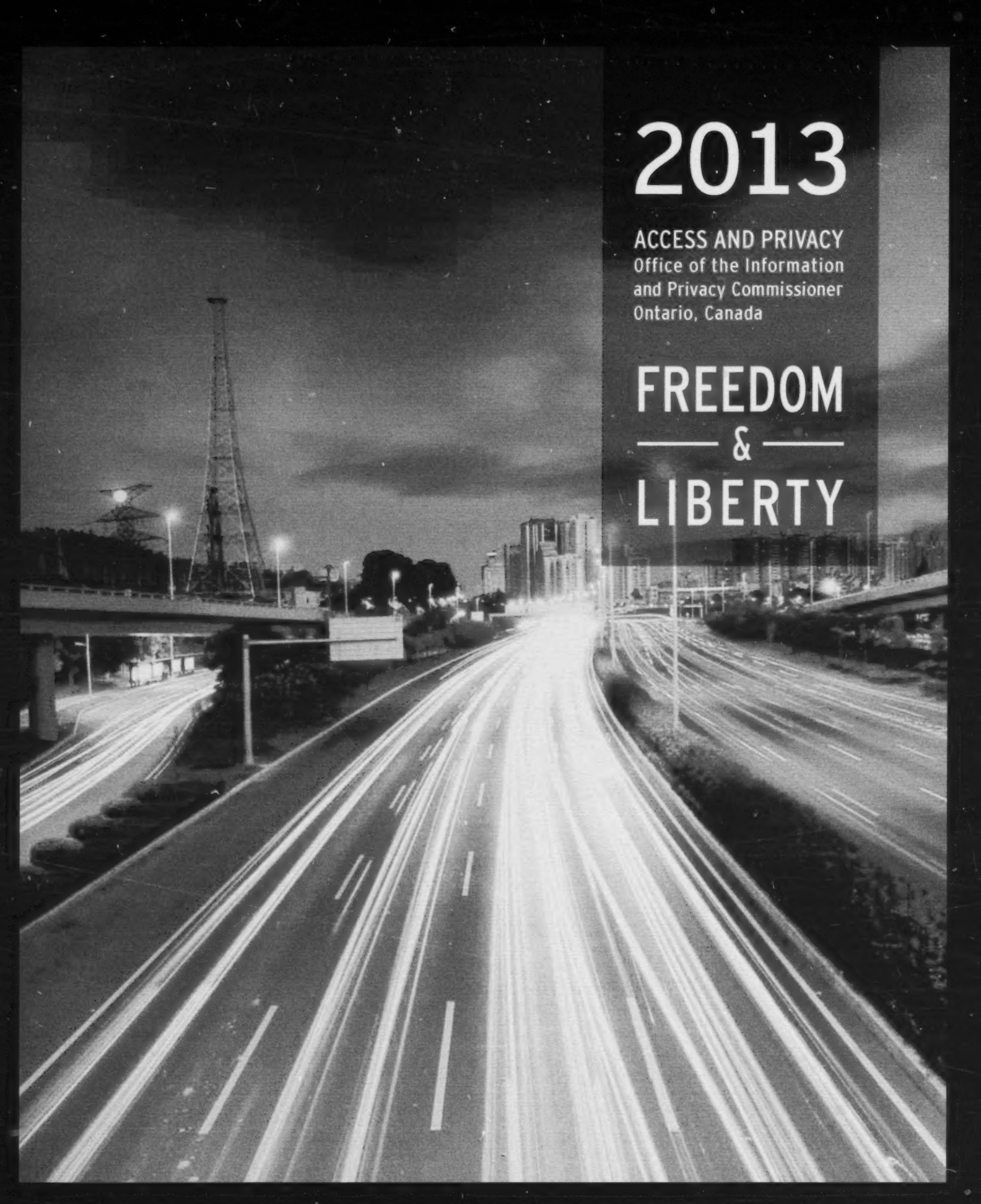
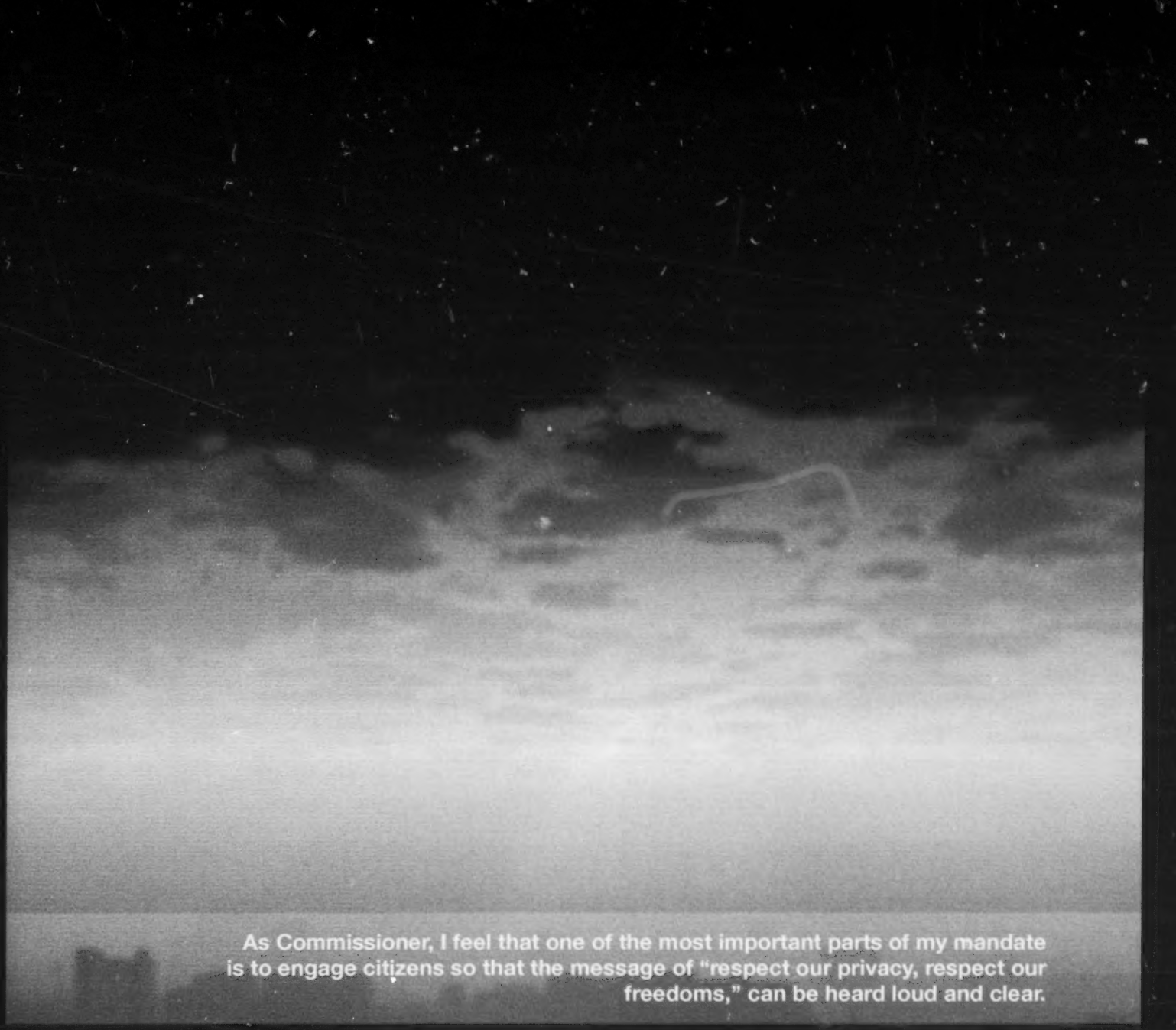

2013
ACCESS AND PRIVACY
Office of the Information
and Privacy Commissioner
Ontario, Canada
FREEDOM
&
LIBERTY



As Commissioner, I feel that one of the most important parts of my mandate is to engage citizens so that the message of "respect our privacy, respect our freedoms," can be heard loud and clear.

COMMISSIONER'S MESSAGE

WHEN I BEGAN MY FIRST TERM AS ONTARIO'S INFORMATION AND PRIVACY COMMISSIONER IN 1997, I COULD NOT HAVE IMAGINED HOW MUCH THE WORLD WOULD BE CHANGING! Computers and the Internet were still largely limited to desktops in homes and offices. Laptops were still unwieldy devices, and cellphones were still a long way from becoming "smart."

Today, information technology is compact, mobile, and everywhere. You cannot walk down the street without seeing someone using some sort of mobile device that has more computing power than an office floor full of computers, just a generation ago. There is almost no aspect of our lives left that remains untouched by information and communications technology.

When I was reappointed for a second term in 2004, I stated that we were in the midst of profound change in the areas of privacy protection and access to government information. However, as I have always maintained, technology – which has resulted in many challenges – can also be tapped for innovative solutions, particularly for privacy and access.

I was deeply honoured when the Legislative Assembly of Ontario reappointed me again in 2009, to serve as Commissioner for an unprecedented third term. It is a day I will never forget and I am still deeply grateful to the Members of Provincial Parliament for their strong support and confidence. I pledged that I would focus on *Privacy by Design*, and to promote government transparency and accountability through our newly developed *Access by Design*.

As evidenced by the chronology of examples below, I believe that we've accomplished a lot since then, not only for the residents of Ontario, but also for future generations both here at home, and around the world.

2009

In 2009, I continued to advance *Privacy by Design* on the world stage by launching *The 7 Foundational Principles* of *Privacy by Design*, which I am proud to say have now been translated into 35 languages, with more to come. To ensure that *Privacy by Design* continued to gain strong global momentum, I also launched **www.privacybydesign.ca** as a repository of news, information and research.

In an entirely different area, following an extensive investigation, I issued a special report entitled, *Excessive Background Checks Conducted on Prospective Jurors: A Special Investigation Report*. As part of my recommendations, I ordered Crown attorneys to cease collecting any personal information of potential jurors, beyond that which was necessary under the *Juries Act* and Criminal Code. I also proposed a fundamental shift in the way that prospective jurors were screened. The new process addressed the lack of consistency in the "patchwork of practices" employed by Crown attorney offices and the police.

2010

I launched a campaign called, Stop.Think.Protect. which appealed to Ontario's health sector to help combat the growing number of avoidable breaches involving personal health information. Specifically, health-care organizations were asked to educate their staff on the simple steps required to prevent the far too frequent disclosure of unencrypted data through the loss or theft of portable electronic devices.

A landmark resolution was unanimously passed in Jerusalem by the International Assembly of

Privacy Commissioners and Data Protection Regulators, recognizing *Privacy by Design* as an essential component of fundamental privacy protection – transforming it overnight into an international standard.

I unveiled my concept of *Access by Design*, consisting of *7 Fundamental Principles* that encourage public institutions to take a proactive approach to releasing government records, making the disclosure of government-held information an automatic process wherever possible – i.e., access as the default.

2011

I declared 2011 as my personal "Year of the Engineer," reaching out to those who design and build the systems and technologies upon which we rely. I wanted to challenge every innovator and engineer to operationalize *Privacy by Design* and make it an everyday reality. I was delighted by their response to my message and their willingness to take up the challenge to make privacy the default condition. It became clear that this was eminently "doable!"

The Ontario Lottery and Gaming Corporation (OLG) launched its voluntary self-exclusion program following a successful collaboration with my office and the University of Toronto. This program sought to embed a design protocol based on *Privacy by Design* called Biometric Encryption. This enabled the OLG to better support its customers who had enrolled in a completely voluntary self-exclusion program, while protecting the personal data of all OLG customers.

2012

I held a public symposium called, *Beware of "Surveillance by Design:" Standing up for Freedom and Privacy*, bringing together a highly respected panel of thought leaders to share their perspectives and raise awareness of the serious privacy implications of proposed federal "lawful access" legislation [there was nothing lawful about it]. I was gratified when people from across the political and social spectrum rallied to the defence of privacy in response to the government introducing Bill C-30, a highly privacy-invasive piece of legislation. We were successful in the bill ultimately being withdrawn.

After a long campaign, the *Broader Public Sector Accountability Act* came into effect, bringing Ontario's hospitals under the *Freedom of Information and Protection of Privacy Act*. This was a historical milestone in the evolution of freedom of information in Ontario, allowing citizens the right to make a request for access to a range of recorded information.

Over the course of my investigation into Elections Ontario's loss of two USB keys, containing the unencrypted personal information of as many as 2.4 million voters, I found the cause could be traced back to the agency's failure to systemically address privacy and security issues. I recommended that Elections Ontario take concrete steps in three areas to enhance the protection of personal information – policies, practices, and procedures; training and compliance; as well as accountability. The Chief Electoral Officer for the province accepted my recommendations unreservedly. As a companion to my report, I also released a guidance document, *A Policy is Not Enough: It Must be Reflected in Concrete Practices*, on how to effectively execute an appropriate privacy policy and embed it in the concrete practices of an organization.

ORION Think Conference - Hon. Reza Moridi, Minister of Research and Innovation; Dr. Ann Cavoukian, Information and Privacy Commissioner, Ontario; Darin Graham, President and CEO, ORION

Privacy by Design User Forum

In order to guide organizations through the implementation of *Privacy by Design*, I released a groundbreaking paper, *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices*. The paper provided an anthology of the experiences of organizations from a wide range of sectors, including telecommunications, technology, health care, transportation, and energy. It also provided a comprehensive overview of the partnerships and joint projects that I have engaged in to implement *Privacy by Design*, by providing concrete and meaningful operational effect to its principles.

2013

In my 2012 Annual Report, I said that the key question for 2013 would be whether Bill C-30, so-called "lawful access" legislation, would be amended to incorporate privacy protections. I learned the answer to that in early 2013, and I was absolutely delighted. On February 11, 2013, the federal government announced that it would not proceed with Bill C-30, and any attempts to modernize the Criminal Code will not contain the measures in Bill C-30, including the warrantless mandatory disclosure of basic subscriber information, or the requirement for telecommunication service providers to build intercept capability within their systems. Privacy and freedom would survive for another day!

However, the feeling of success that came with the demise of Bill C-30 would not last long. In November, the federal government introduced Bill C-13, which would enact new surveillance powers again under the guise of protecting children. While not as heavy-handed as its predecessor, Bill C-30, this new bill nevertheless leverages new and evolving surveillance technologies which pose a threat to the privacy rights of every Canadian. As Commissioner, I feel that one of the most important parts of my mandate is to engage citizens so that the message of "respect

our privacy, respect our freedoms," can be heard loud and clear.

Adding further ammunition to an already troubling year for privacy, Edward Snowden, a former analyst with the U.S. National Security Agency (NSA), came forward to reveal just how invasive, and pervasive, government surveillance was in the lives of everyday citizens. Further, it would also come to light that the NSA was not acting alone. These revelations brought to light the involvement of major information and technology companies, as well as the remaining "Five Eyes" countries, comprised of the United Kingdom, Australia, New Zealand and Canada's Communications Security Establishment (CSEC). Prompted by what I believed to be a global assault on privacy with no government accountability, I published a joint op-ed with Ron Deibert, Andrew Clement and Nathalie Des Rosiers in the Globe and Mail entitled, *Real Privacy Means Oversight.* The main point of the article was that in free and democratic societies, governments must be accessible and transparent to their citizens. Further, governments should only be permitted to access personal information when authorized by law. When it comes to the state's power to conduct surveillance, critical privacy protections must include judicial authorization and independent oversight.

In June, I released the findings of my investigation into a complaint by MPP Peter Tabuns, who alleged that the Chief of Staff to the former Minister of Energy had improperly deleted all emails concerning the cancellation of the Mississauga and Oakville gas plants. As recounted in my Special Investigation Report, *Deleting Accountability: Records Management Practices of Political Staff,* I uncovered that at the root of the problem was the practice of the indiscriminate deletion of all emails sent and received by senior political staffers. This practice violated the *Archives and Recordkeeping Act* (*ARA*) and undermined the transparency and accountability purposes of the *Freedom of Information and Protection of Privacy Act* (*FIPPA*). In my Report, I recommended that the government take concrete steps in three specific areas: Office of the Premier and Ministers' Offices; legislative changes; and records retention policies. I am pleased to report that the Premier and the government have made significant progress in addressing each of the recommendations made; my office continues to work closely with them.

The U.S. Federal Trade Commission Chairwoman, Edith Ramirez, stated that the principles of *Privacy by Design* should be adapted to the emerging world of Internet-connected appliances and other devices, given the potential for a new explosion of consumer data collection. Chairwoman Ramirez further suggested that companies should adhere to three core principles espoused by the FTC: building privacy features into new products from the outset – a concept known as *Privacy by Design*; being transparent with consumers about what information devices are collecting and how the information is being used or shared; and giving consumers control over their data.

2014

On January 28, 2014, International Privacy Day, I held a standing-room-only public symposium, *Big Surveillance Demands Big Privacy – Enter Privacy-Protective Surveillance.* More than 400 people registered to attend in person and via webcast to hear highly esteemed speakers from academia, the legal community, and civil society address the numerous issues surrounding state

surveillance, including the urgent need for independent parliamentary oversight.

Most disturbing, on the day of our very successful symposium, I learned that CSEC had used information collected from free Wi-Fi at a major Canadian airport to track the wireless devices of thousands of airline passengers – tracking them for days after they had left the terminal. CSEC claimed that this activity was legal as they were only collecting metadata. I strongly challenged this assertion. These undertakings do not resemble the activities of a free and open society.

Conclusion

There are times when I still cannot believe that twenty-five years have passed since I first joined the Office of the Information and Privacy Commissioner (IPC) – the last sixteen of those gave me the honour of serving as Commissioner. During that time, I have been given so many opportunities to uphold and fight for the causes of privacy and access. I was also fortunate to find myself as Commissioner during a unique historical period when the advent of the Internet would fundamentally change the very concepts of privacy and access. As I have said before, in a perfect world, we would not need the IPC. However, we do not live in a perfect world – far from it, and despite the advances we have made in access and privacy, our efforts are needed now, more than ever. As I look back on the past years of the IPC, I feel that Ontarians can be assured that this office has grown into a first-class agency, known around the world for demonstrating innovation and leadership, in the fields of both access and privacy. If anything, my efforts and the efforts of our office have always been to advance a noble cause – to continually strive for the pursuit of open, transparent government and the protection of our privacy – which lies at the very heart of our free and open society. May this continue well into the future.

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner, Ontario, Canada

As I have said before, in a perfect world, we would not need the IPC. However, we do not live in a perfect world – far from it, and despite the advances we have made in access and privacy, our efforts are needed now, more than ever.

In free and open societies,
governments must be accessible and
transparent to their citizens.

TABLE OF CONTENTS

Commissioner's Message 1
Commissioner's Recommendations..... 11
Privacy by Design 17
Key Issues 23
Call to Action for Canadians 30
Access to Information..... 35
Statistics..... 41
Financial Statement ..... IBC

Around the world, governments are strengthening laws to meet the realities of the 21st century. We must do the same to ensure that Ontario remains a leader in access and privacy.

COMMISSIONER'S RECOMMENDATIONS

Modernization of *FIPPA* and *MFIPPA*

It has now been more than 20 years since the *Freedom of Information and Protection of Privacy Act* (*FIPPA*) and the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*) came into effect, and both could now be considered mature legislation. When the *Acts* were originally being debated, legislators could not have envisioned the vast opportunities and challenges that have arisen through the explosive growth of the Internet, the Web, and now, the world of Big Data. As a result, they no longer reflect the realities of access to information and the protection of privacy by public institutions in the Information Age. In addition, Edward Snowden's revelations about government surveillance programs have heightened Canadians' concerns about the erosion of their privacy, prompting calls for increased transparency and greater oversight. Around the world, governments are strengthening laws to meet the realities of the 21st century. We must do the same to ensure that Ontario remains a leader in access and privacy.

This past October, I supported a joint resolution by federal, provincial and territorial Information and Privacy Commissioners urging governments across the country to update their access and privacy laws. I felt it was imperative for the Ontario government to undertake a comprehensive review of the *Acts* in order to modernize the legislation. I strongly believe the following reforms, among others, should be considered:

- Providing strong enforcement powers and penalties for non-compliance with the privacy provisions of the *Acts*;
- Strengthening reporting requirements to the public with respect to the disclosure of personal information between public and private entities;
- Creating new systems and incentives for proactively embedding privacy at the design stage of information technologies and operational processes; and
- Establishing of more systems for the proactive disclosure of information.

Children's Aid Societies

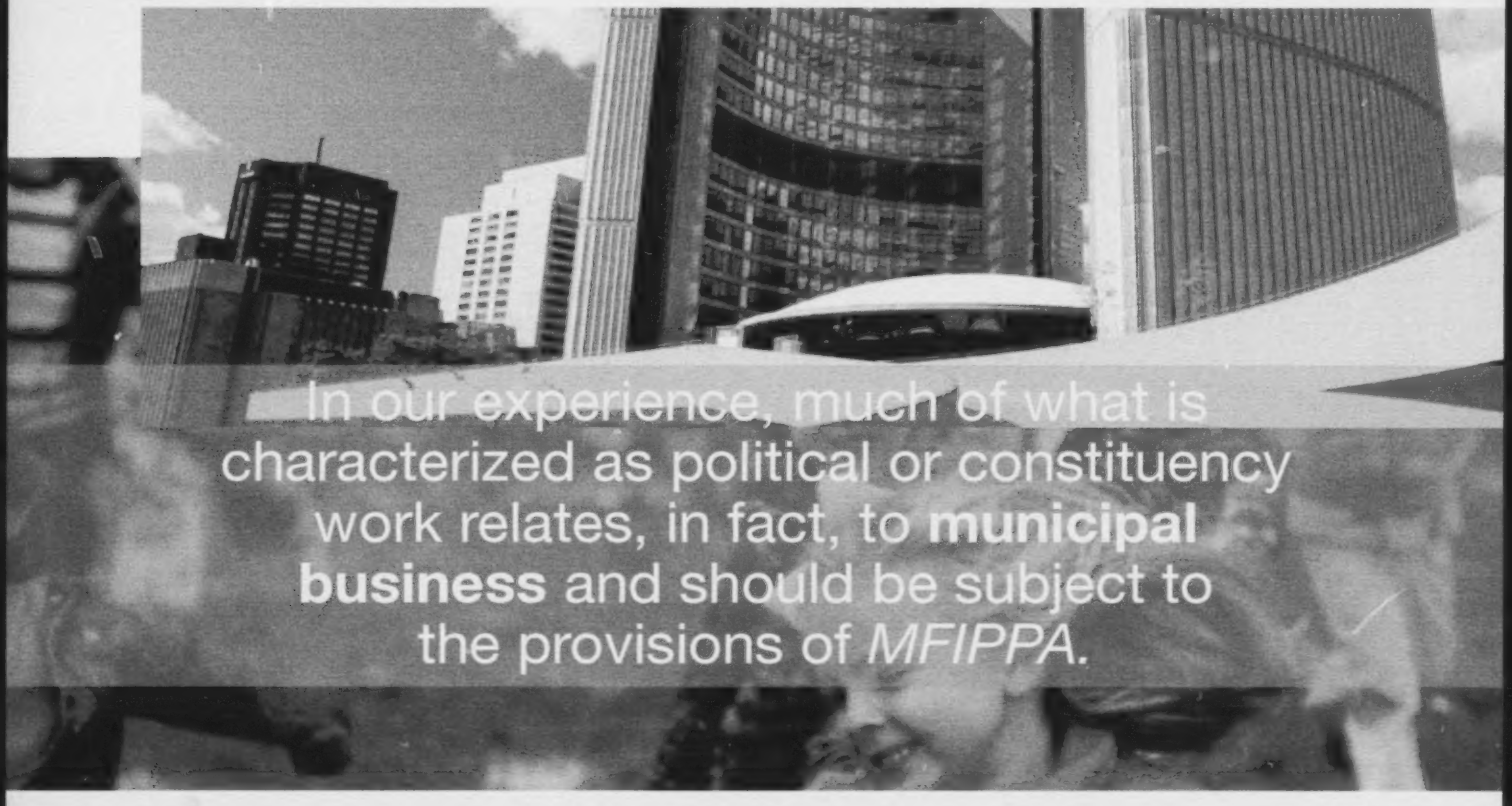
In my 2004, 2009, and 2012 Annual Reports I recommended that Children's Aid Societies, which provide services for some of our most vulnerable citizens – children and youth in government care, be brought under *FIPPA*. I am disheartened by the complete lack of action to ensure transparency and accountability by these organizations that received significant public funding. As part of the modernization of the *Acts*, I call on the government to finally address this glaring omission and ensure that Children's Aid Societies are added to the list of institutions covered.

Municipal Councillors' Records

When freedom of information requests are made for records in the possession of municipal councillors, traditionally there has been a distinction made between constituency records and those records that were created while the councillor was conducting business on behalf of the municipality. In practice, this has not worked well. In our experience, much of what is characterized as political or constituency work relates, in fact, to municipal business and should be subject to the provisions of *MFIPPA*.

This issue has received a great deal of attention as a result of access requests for records held by City of Toronto councillors. Several of our recent orders have found that based on the current wording of the *Act*, the requested records were not within the custody or control of the City, so they were not subject to an access request. Unfortunately, this does not meet the public's demands for transparency and accountability. When it comes to the expenditure of taxpayer dollars, there are many valid reasons why information such as travel, hospitality and other expenses of municipal councillors should be made publicly accessible.

This past year, I wrote to both the Minister of Government Services and the Minister of Municipal Affairs and Housing asking the provincial government to study possible amendments to *MFIPPA* to clarify the status of the records of municipal councillors. I understand that work has been undertaken in this regard. I feel very strongly that these amendments are necessary to further open up government records to the public and encourage greater trust.


In our experience, much of what is characterized as political or constituency work relates, in fact, to **municipal business** and should be subject to the provisions of *MFIPPA*.

Government Contracts

Each year we receive a number of appeals dealing with requests for contracts awarded by public institutions. These agreements can range from the building of new infrastructure projects to outsourcing services such as waste management, snow removal, and housekeeping. Contracts awarded by institutions represent significant government spending of taxpayer money, so transparency is vital. Ontarians have a right to know how their money is being spent.

I have repeatedly called for publicly funded contracts to be disclosed routinely and proactively. This regular disclosure would strengthen transparency and accountability around government spending and improve public confidence. It would also significantly reduce the number of freedom of information requests submitted to government and appeals handled by my office. I am pleased to report that there are institutions who have heeded my call. For example, I believe the City of Toronto has set an example for others to consider.

Unfortunately, many requesters continue to experience difficulty in accessing government contracts. There are institutions that are denying freedom of information requests for contracts using sections of *FIPPA* and *MFIPPA* relating to third party information. These sections are also routinely used by contracting parties to require requests to go through the appeal process in my office, thus needlessly delaying the release of contracts.

I call on the government to amend the *Acts* to provide clarity to the sections being used to deny access to these records and send a clear message that this information should proactively be made available to the public, without the need to resort to the freedom of information process.

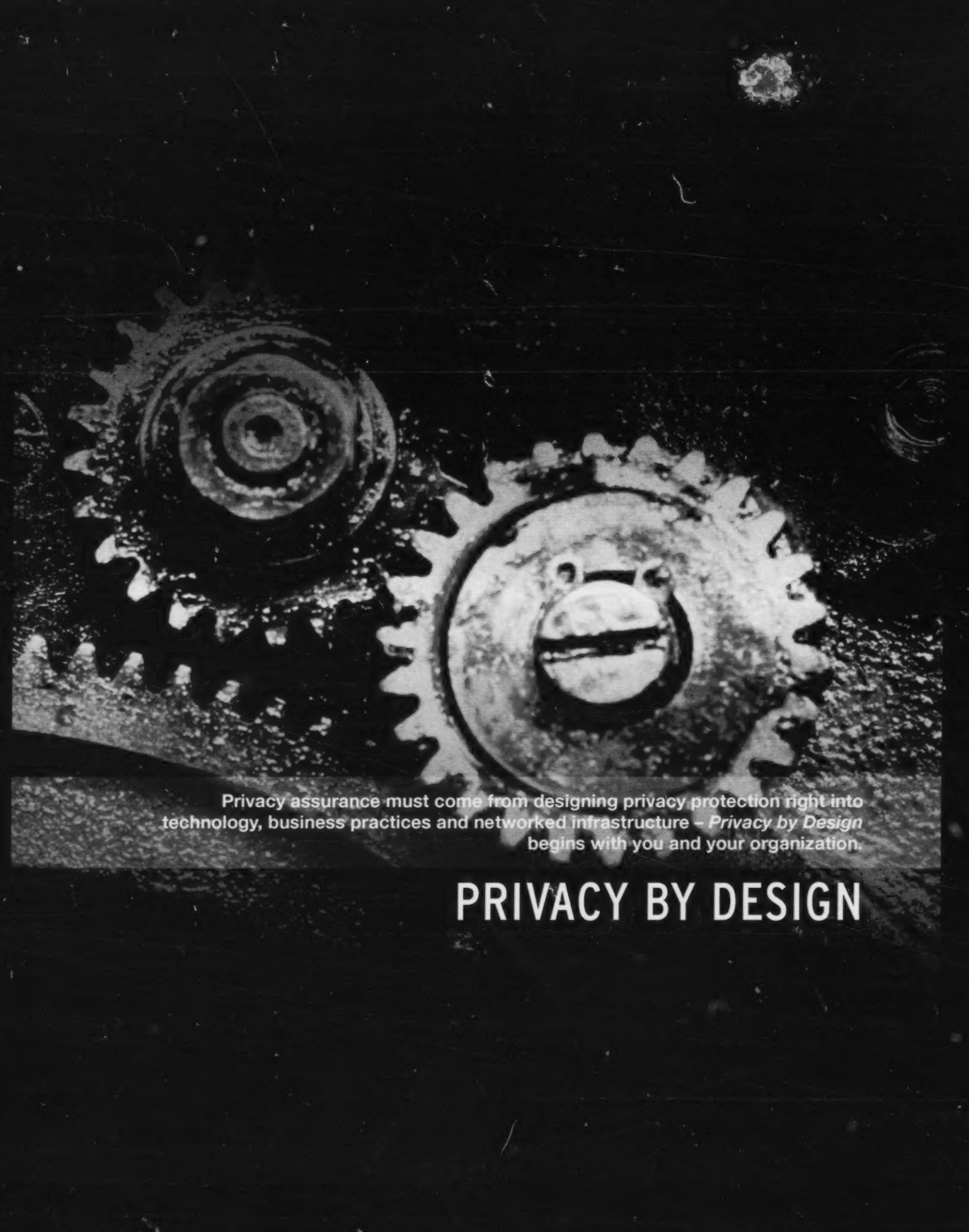
The challenge we face is that there are currently
no consequences for poor records
management practices or the wilful destruction of
records, and I feel that this must be changed.

New Consequences for Insufficient Record Retention

My Special Investigation Report, *Deleting Accountability: Records Management Practices of Political Staff*, found both a lack of understanding and concern within government regarding the vital need to retain relevant business records. My office and our freedom of information legislation can only serve the public effectively if appropriate records are kept and key decisions are fully documented. The challenge we face is that there are currently **no** consequences for poor records management practices or the wilful destruction of records, and I feel that this must be changed. For the government to remain transparent and accountable, the expectations for record-keeping must be raised, education on the duty to document must be implemented throughout the government, the consequences for not keeping appropriate business records must be increased, and most importantly, it should be an offence to wilfully destroy records.

Therefore, my four key recommendations are:

1. Create a legislative duty to document business-related activities within *FIPPA* and *MFIPPA*, including a duty to accurately record key decisions;
2. Require that every institution subject to *FIPPA* and *MFIPPA* put in place reasonable measures to securely retain records that are subject to, or may reasonably be subject to, an access request under *FIPPA* and *MFIPPA*.
3. Prohibit the wilful destruction or alteration of records that are subject to, or may reasonably be subject to, an access request under *FIPPA* and *MFIPPA*; and
4. Make it an offence under *FIPPA* and *MFIPPA* for any person to wilfully destroy or alter records that are subject to, or may reasonably be subject to, an access request under *FIPPA* and *MFIPPA*.



Privacy assurance must come from designing privacy protection right into technology, business practices and networked infrastructure – *Privacy by Design* begins with you and your organization.

PRIVACY BY DESIGN

Dr. Ann Cavoukian, Information and Privacy Commissioner, Ontario, is recognized as an Honorary Architect at the *Privacy by Design* User Forum by Drummond Reed, CEO, Respect Network; Becky Burr, Chief Privacy Officer, Neustar; Gary Rowe, Executive Chairman, Respect Network; Mark Black, CEO, The Trusted Cloud Company; and Les Chasen, VP of Technology Strategy, Neustar.

Privacy by Design Ambassadors

In 2013, we saw a significant increase in the number of *Privacy by Design* (*PbD*) Ambassadors. There are now over 200 individual *PbD* Ambassadors from all over the world – individuals who advance the case for embedding privacy-protective measures in technology, processes, and networked infrastructure. This exclusive, but growing, group of privacy thought leaders are comprised of industry experts, entrepreneurs, academics, engineers, innovators, lawyers, and C-level executives.

The same trend is evident with our Organizational *PbD* Ambassadors. We have doubled our Organizational Ambassadors – comprised of organizations that embed the 7 Foundational Principles of *Privacy by Design*, not just into selected projects, but into the very operation of the organization itself. As with individual *PbD* Ambassadors, the reach has been global and varied. Organizational Ambassadors deliver products and services across a wide array of sectors such as health care, technology, Cloud Computing, energy, and biometrics. I have been extremely pleased to see the *PbD* Ambassador community growing. It reinforces that *Privacy by Design* is the gold standard of commitment to the protection of personal information.

PbD

www.privacybydesign.ca

Privacy by Design Centre of Excellence

Privacy by Design
Centre of Excellence

PbD Ontario

April 15, 2013 marked the launch of the *Privacy by Design* Centre of Excellence, a joint initiative of the Ministry of Government Services (MGS) and the Office of the Information and Privacy Commissioner (IPC). The *PbD* Centre of Excellence was established to provide resources and guidance to more than 65,000 Ontario Public Service (OPS) members. Since April, the Centre of Excellence has expanded its reach beyond the OPS and has seen increased involvement from the Broader Public Sector (BPS), such as hospitals, municipalities and academic institutions.

The *PbD* Centre of Excellence engages a broad spectrum of professionals in improving privacy protection practices, such that they are better able to identify emerging issues, enhance the collective understanding of common practices, and educate the community. With this in mind, we can ensure that privacy continues to be embedded as the default in both new and existing Ontario government programs. The formal adoption of *PbD* across all levels of government will undoubtedly secure Ontario's place as a world-class leader in privacy protection for years to come and I look forward to seeing new and innovative ways of integrating *PbD* into the technology, business practices, and physical design of our communities.

New *Privacy by Design* Papers

Privacy and Security by Design: A Convergence of Paradigms highlights the convergence of a common "design-thinking" perspective between privacy and security. The paper explores how security and privacy share notable similarities and how they may complement and mutually reinforce each other.

Privacy by Design and Third Party Access to Customer Energy Usage Data explores the issue of third party access to Customer Energy Usage Data and its benefits, as well as potential privacy risks. It examines potential new products and services created by third party access, which may support conservation and new market opportunities.

Looking Forward: De-identification Developments — New Tools, New Challenges provides an update on recent de-identification developments and looks ahead to new, up-and-coming issues related to the topic of de-identification.

A proactive *Privacy by Design* approach is central to designing and implementing the regulatory framework needed to properly supervise state surveillance using new technologies. ***Surveillance, Then and Now: Securing Privacy in Public Spaces*** provides resources to aid law enforcement, lawmakers, and the broader public in understanding and protecting our fundamental right to privacy of our activities in public spaces.

A Primer on Metadata: Separating Fact from Fiction rebuts the popular claim that the information on personal communications being seized by government agencies—above all, the U.S. National Security Agency (NSA)—is neither sensitive, nor privacy-invasive, since it is "only metadata." The paper calls for proactive measures designed to enable both privacy and security and for greater accountability, oversight, and transparency on the part of government agencies.

In ***Privacy by Design: Fundamentals for Smart Grid App Developers***, we reach out to Smart Grid app developers by providing a primer on *Privacy by Design*. By employing the principles, not only will customers trust apps, but the application devel-

A **proactive** *Privacy by Design* approach is central to designing and implementing the regulatory framework needed to **properly supervise** state surveillance using new technologies.
look forward to seeing new and innovative
business practices, and physical design

oper will also stand out as an early adopter — leading with privacy in Smart Grid apps — by design.

Introducing Privacy-Protective Surveillance: Achieving Privacy and Effective Counter-Terrorism illustrates the organizing methodology behind PPS and demonstrates that contrary to appearances, it is possible to have both privacy and effective counter-terrorism. We have state of the art technologies and can develop the system to achieve this — a win-win proposition!

As threat levels rise, the old way of protecting data assets, which simply builds a defensive "perimeter" around a resource, will no longer be sufficient. ***Privacy and Security by Design: An Enterprise Architecture Approach*** illustrates how security must go on the offensive and address information security and privacy concerns as the default mode of operation of a business or organization.

Personal Data Ecosystem (PDE) — A Privacy by Design Approach to an Individual's Pursuit of Radical Control explores the emerging landscape of companies and organizations that believe individuals should be in control of their personal data and make available a growing number of tools and technologies to enable this control.

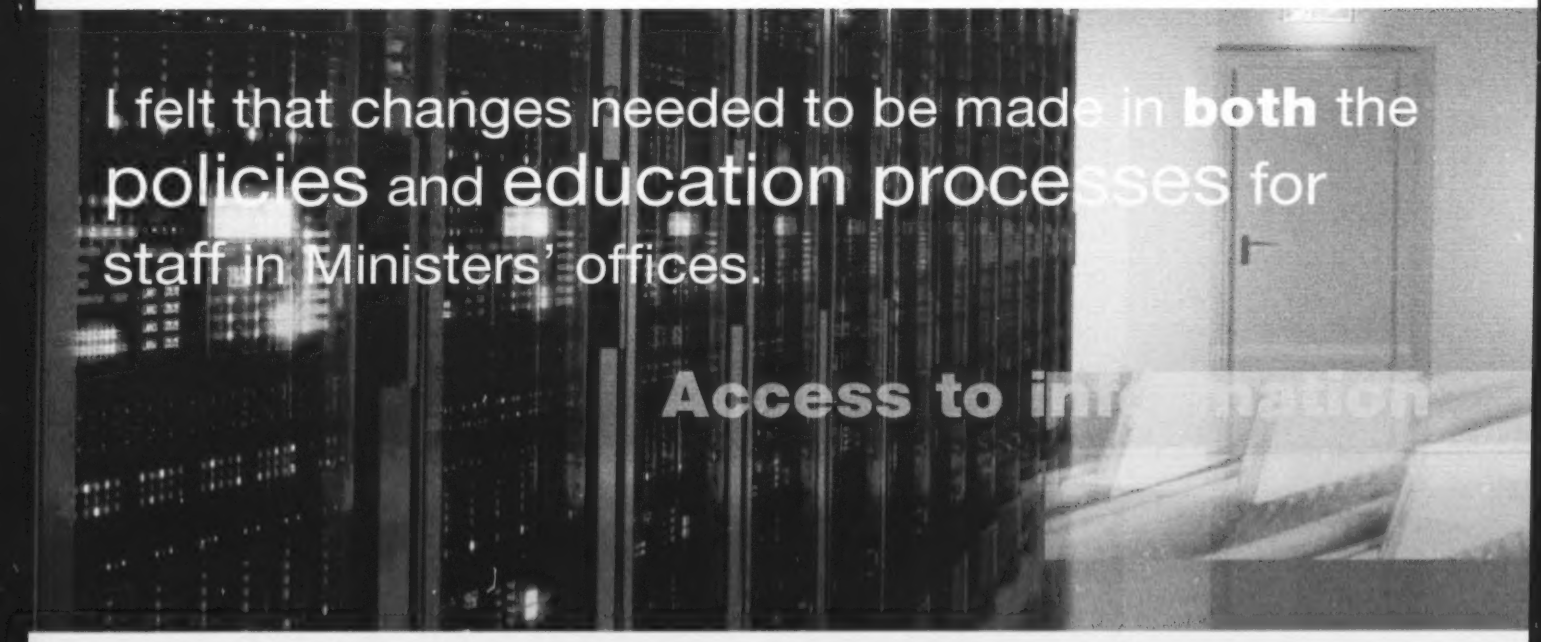
Privacy Exposures and Risk Reduction Strategies for Small Organizations reinforces the notion that privacy policies and procedures alone, without a concrete strategy for implementation, will not protect an organization from privacy risks. Applying the basic concepts of *Privacy by Design* in a small enterprise setting is essential to avoiding the pitfalls of harmful data leaks.

Big Privacy: Bridging Big Data and the Personal Data Ecosystem Through Privacy by Design defines the seven architectural elements of Big Privacy and illustrates how they apply to the unique challenges of Big Data environments in the context of a Personal Data Ecosystem.

Consistent with the *Privacy by Design* principle of comprehensive end-to-end security, ***BYOD: (Bring Your Own Device) Is Your Organization Ready?*** examines information management risks and offers practical implementation guidance to mitigate them. While no one-size-fits-all solution exists, the paper sets out a comprehensive five-step process for organizations to achieve both privacy and security in a BYOD program.

We can, and must, have both security and privacy, in unison. It should not be one at the expense of the other.

KEY ISSUES


I felt that changes needed to be made in **both** the
policies and education processes for
staff in Ministers' offices.
Access to information

Special Investigation – Deleting Accountability: Record Management Practices of Political Staff

Access to information is key to a free and democratic society. It allows citizens to know about the activities of government and understand how the public's money is being spent. Without a written record of how key government decisions are made, transparency is undermined and the basis for policy choices may be shielded from public scrutiny.

This past year, my office was faced with the unfortunate task of investigating the record keeping practices of key members of both the former Premier's and the former Minister of Energy's offices. Our investigation was initiated in April immediately after receiving a complaint from a Member of Provincial Parliament. The allegation was that the former Chief of Staff to the Minister of Energy had improperly deleted all emails pertaining to the cancellation and relocation of the Oakville and Mississauga gas plants. Of significance was the fact that despite more than 56,500 pages of responsive records having been produced to a Legislative Committee studying the gas plant issue by the Ministry of Energy and the Ontario Power Authority (OPA), not one responsive record was produced by political staff in the Minister of Energy's office.

In an interview with the former Chief of Staff, he informed us it was his practice to routinely delete all emails. The reasoning was that he liked to maintain a "clean inbox" policy. It was difficult to accept that the routine deletion of emails was not, in fact, an attempt to avoid transparency and accountability in relation to his work. Further, I had trouble accepting that this practice was simply part of a benign attempt to efficiently manage one's email accounts.

During the course of the interviews we conducted as part of our investigation, we met with the Secretary of the Cabinet. We learned

that in early 2013, when the former Premier's staff was preparing for the transition to the new Premier, the former Premier's Chief of Staff approached him, asking questions about "how to wipe clean the hard drives in the Premier's office." While the Secretary took steps to inform him of their obligations, I was concerned that the inappropriate deletion of electronic records by political staff in the former Premier's office may have taken place. As a result, I decided to expand the scope of my investigation.

During discussions with the Chief of Staff to the former Premier, I learned that he had a similar policy of deleting his emails daily. Although I cannot say with complete certainty that there was an improper deletion of electronic records from computer hard drives by the former Premier's staff in the transition to the new Premier, their email management practices indicated, at a minimum, a failure to meet the record keeping responsibilities.

The investigation led us to in-depth discussions with the Ministry of Government Services (MGS) about how electronic information and emails were stored and saved. We had hoped it was possible to recover the deleted email records; however, we were told that these records had been permanently deleted and recovery would not be reasonably possible.

Upon reflection on the issues raised by this investigation and the evidence we gathered, I became very concerned with the apparent lack of responsibility and accountability for records management practices within the offices of senior political leaders in this province. There was no doubt that the email management practices of both the former Minister's office and the former Premier's office had violated the *Archives and Recordkeeping Act* (*ARA*) and the records retention schedule developed for ministers' offices by the Archives of Ontario.

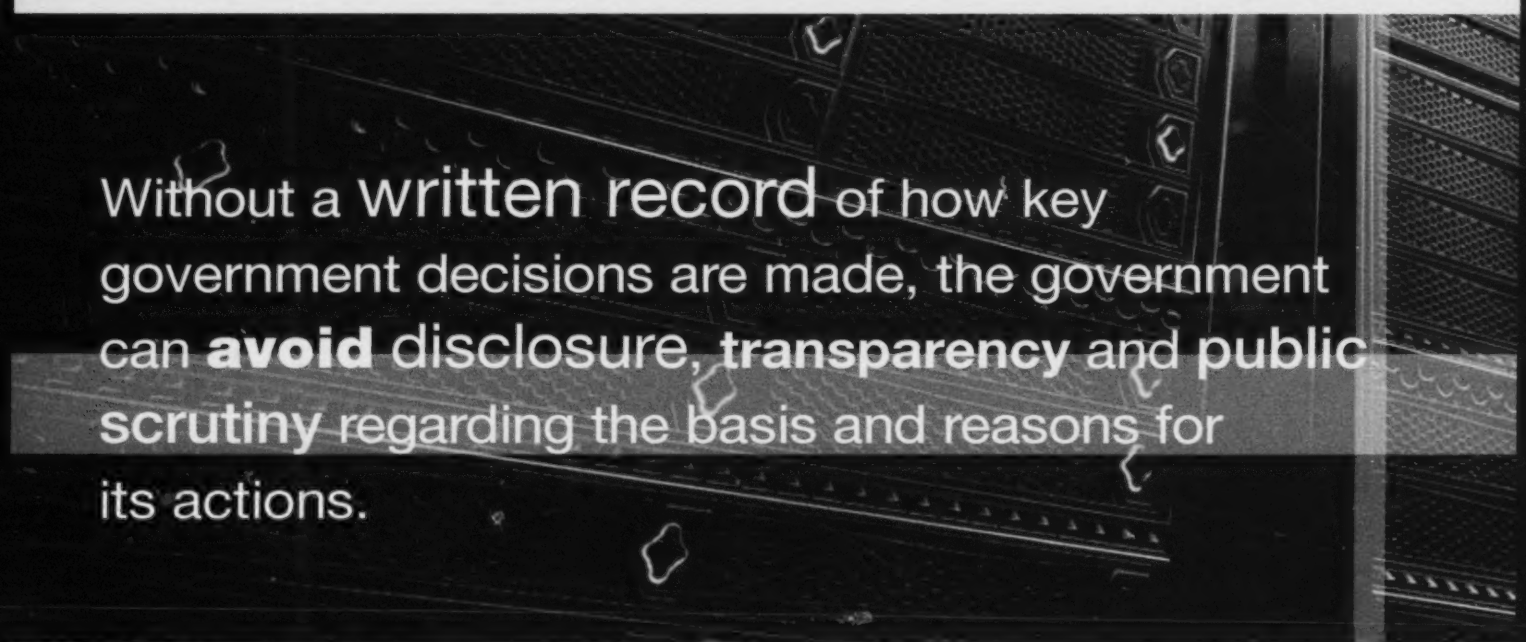
This practice also undermined the principle of the public's right of access to government records under the *Freedom of Information and Protection of Privacy Act* (*FIPPA*), in addition to the transparency and accountability principles that form the foundation of both these *Acts*. I felt that changes needed to be made in both the policies and education processes for staff in Ministers' offices. Also, I was concerned that there was no designat-

ed person in the offices of the former Premier and former Minister of Energy who was accountable for records management practices or to ensure that political staff were aware of their obligations.

In my Report, *Deleting Accountability: Records Management Practices of Political Staff*, which was released in June, I recommended that the government take concrete steps in three specific areas to ensure that records that may be subject to an access request under *FIPPA* and the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*) are retained:

- Office of the Premier – Issue a directive requiring that a senior official in each minister's office and the Premier's office be designated as the person who is accountable for records retention policies and practices, and for ensuring that political staff receive training on their records management obligations.
- Legislative Changes – Amend both *FIPPA* and *MFIPPA* to address institutions' responsibilities to ensure that all key decisions are documented and records securely retained – making it a serious offence to wilfully and inappropriately destroy records.
- Records Retention Policies – Conduct a review of the Archives of Ontario records retention policies and practices that apply to the records management processes in ministers' offices and the Premier's office, ensuring that responsibility for retaining official or business records is clearly set out.

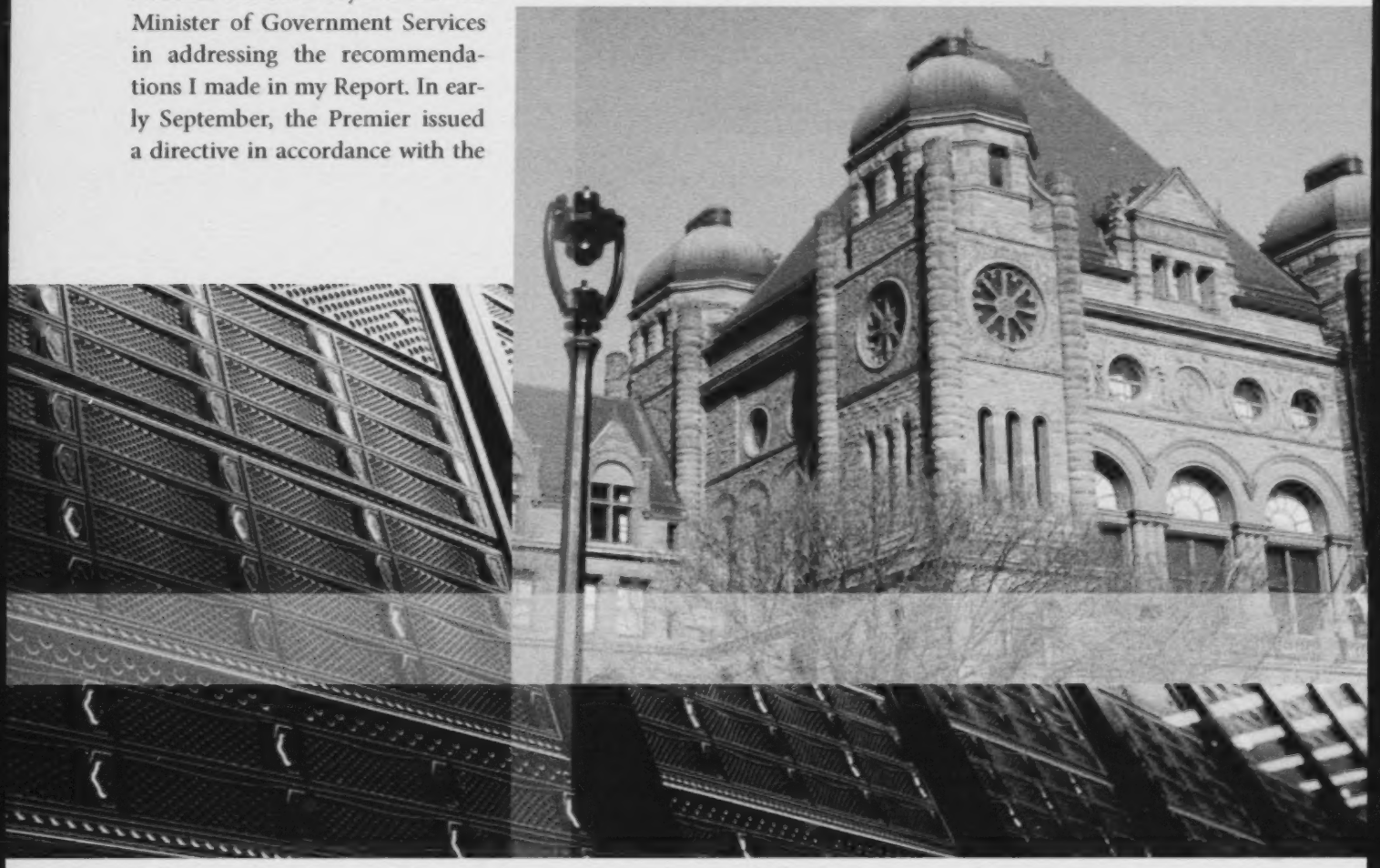
Subsequent to the release of my Report, I was provided new information about the Ontario Public Service's email system – details which should have been provided to me during my investigation. In addition, I learned that the MGS had failed to "look under the hood" and conduct an appropriate forensic investigation when asked about recovering deleted emails. Ministry staff trusted that their information management process had worked correctly and that the emails were permanently deleted. I had faith that MGS had done the necessary work to arrive at this conclusion and accepted their response. Only in response to the motions of the Standing Committee on Justice Policy did ministry staff complete the necessary due diligence and go beyond mere reliance on policy. I was dismayed to learn that we had


Without a written record of how key government decisions are made, the government can avoid disclosure, transparency and public scrutiny regarding the basis and reasons for its actions.

been provided with incorrect information; however, pleased that additional records had been found. As a result, I released an Addendum to my report in August describing the circumstances surrounding the disclosure of this new information. I noted that the Deputy Minister for MGS had apologized to me and assumed full responsibility. These events and the new information did not impact the recommendations in my initial Report – they were still valid and remained unchanged.

Since the conclusion of my investigation, I have appreciated the cooperation I have received from Premier Kathleen Wynne and the Minister of Government Services in addressing the recommendations I made in my Report. In early September, the Premier issued a directive in accordance with the recommendations made in the Report and committed the government to greater transparency and accountability through much improved record keeping practices. In addition, political staff received in-depth training on their record retention responsibilities. I applaud these developments. I look forward to reviewing the forthcoming results of their research into my specific recommendations for legislative amendments.

Without a written record of how key government decisions are made, the government can avoid disclosure, transparency and public scrutiny regarding the basis and reasons for its actions. If the public is deprived of such scrutiny, there can be little accountability, which jeopardizes our free and democratic process. These actions also impede the public's ability to participate in an informed and meaningful way in the democratic process and erode the public's trust in government. I hope that through the implementation of these recommendations, records of key government decisions will be properly kept in the future, and that an investigation of this nature will never be needed again.



Mass Surveillance: The Battle for Transparency and Privacy–Protective Measures

This year propelled surveillance issues and the collection of metadata to the front page. The revelations brought forward by Edward Snowden demonstrated that even more than Americans, Canadians are being the kept in the dark about the activities of our government. We know startlingly little about what our government is doing – and, what foreign intelligence agencies are doing – with our personal information. It is disturbing that there has been so little debate on this important issue, particularly in Parliament. These revelations required both public education and significant action. My office took up the challenge and promoted the immediate need for a full and frank national debate.

The year actually began with a true victory for privacy and freedom. The federal government confirmed that Bill C-30, the proposed legislation which would have allowed police warrantless access to subscriber information, was dead. In recent years, I had spoken out numerous times about how this bill would have infringed on the privacy rights of Canadians, including in relation to their online and mobile activities.

I then turned my attention to the important issue of the growth of surveillance of the public through new technologies. The sustained monitoring of people engaged in everyday activities in public spaces was, in Justice Gerard La Forest's unforgettable words, "an unthinkable prospect in a free and open society such as ours." Days before the Snowden revelations, we introduced a new white paper, *Surveillance, Then and Now: Securing Privacy in Public Spaces*. The purpose of this paper is to assist law enforcement, lawmakers, and the broader public in understanding and protecting our fundamental right to privacy, with respect to surveillance, by the state, of our online and public activities through the use of ever-growing new technologies. It outlines that a proactive *Privacy by Design* approach is central to designing and implementing the regulatory framework needed to properly supervise state surveillance of the public.

In the weeks and months that followed, thanks to Edward Snowden, it became clear that the privacy concerns were much greater than we could have ever conceived. The sweeping surveillance and collection of the public's communication data are a significant threat to privacy and civil liberties. However, various members of the media and the government discounted this information as "only metadata" or simply offered little explanation of its meaning. I set forth to issue, *A Primer on Metadata: Separating Fact from Fiction,* to clearly explain that metadata can actually be more revealing than accessing the content of our communications. The paper aims to provide a clear understanding of metadata and disputes popular claims that the information being captured is neither sensitive, nor privacy-invasive, since it does not access any content. Issued in July, I wrote an opinion piece published in the Toronto Star on the day of its release, highlighting the primer's major points.

As the revelations continued, and the Communications Security Establishment Canada (CSEC)'s involvement became clearer, my office worked to raise awareness of the urgent need for proper oversight. With my co-authors Ron Deibert, Andrew Clement and Nathalie Des Rosiers, we wrote an op-ed published in the Globe and Mail entitled, *Real Privacy Means Oversight*, calling for appropriate parliamentary debate and announced a public symposium scheduled for International Privacy Day, January 28, 2014. The symposium's aim is to explore new ways forward, encouraging a more open dialogue with all security and intelligence organizations, and most importantly, with the public.

As a solution to this complex problem, I worked with Professor Khaled El Emam on a new concept for surveillance – Privacy-Protective Surveillance (PPS). Introduced in early September, the methodology offers a positive-sum (the opposite of zero-sum) alternative to current counter-terrorism surveillance systems. Most measures to counteract terrorism seek to strike a "balance" between public safety and privacy. This often leads to engaging in a zero-sum paradigm of giving up what is perceived to be the "less important value," namely privacy, in favor of the "more significant value," namely public safety. This zero-sum trade-off is invariably destructive in free and open societies. It is not only inappropriate, it is unnecessary. Privacy and counter-terrorism measures can indeed coexist, with both values being respected. We know this is possible to achieve!

Regrettably, the federal government decided late in 2013 to use cyberbullying as an opportunity to resurrect much of its former surveillance legislation, Bill C-30. Thankfully, Bill C-13 does not give police warrantless access to subscriber information, nor does it include Bill C-30's minimum mandatory intercept capacity regime. In addition, most of the proposed powers will be subject to some form of judicial oversight. Nonetheless, C-13's surveillance powers leverage new and still evolving technologies. As a result, they significantly increase, rather than merely maintain, the state's surveillance capacity. Accordingly, I renewed my call for the creation of an independent, arm's length surveillance and review agency, with a strong legislative mandate, to supervise and review state access to the highly sensitive personal information associated with digital communications, as well as report annually to Parliament and the public on the use of surveillance and access powers.

Intrusive proposals require essential matching legislative safeguards - the courts, affected individuals, future Parliaments, and the public must be well informed about the scope, effectiveness, and harms caused by intrusive powers. Properly supervised, domestic surveillance powers can be a valuable tool for security agencies. However, it is equally true that where individuals are subject to unwarranted suspicions, or evidence is poorly handled, or erroneous conclusions are hastily drawn, the consequences for innocent individuals can be devastating. We can, and must, have both security and privacy, in unison. It should not be one at the expense of the other. The true value of privacy must be recognized – and ideally enhanced, not diminished – in any effort to modernize law enforcement powers.

Call to Action

2013 brought a seemingly endless parade of revelations from Edward Snowden about the U.S. National Security Agency (NSA). But what had initially started as an American issue quickly transitioned into a Canadian one, as it became apparent that our own foreign intelligence spy agency, the Communications Security Establishment Canada (CSEC), had been complicit in numerous programs with the NSA, and other "Five Eyes" partners (U.K., Australia and New Zealand). These programs included helping the NSA to create a back door in government-approved encryption tools, making us all more vulnerable to state surveillance. CSEC also aided the NSA in spying at the June 2010 G8 summit in Toronto. In early 2014, we also learned that CSEC's activities included the development of a "game-changing" surveillance tool using metadata associated with persons who used free Wi-Fi at a major Canadian airport. CSEC claimed that this activity was "legal" as they were only collecting "metadata." These assertions were strongly challenged and must continue to be challenged. The collection of metadata can actually be more reveling than accessing the content of the communications.

It has become clear that we have allowed CSEC to operate with even fewer checks and balances than the NSA. CSEC's spying powers represent potential threats to Canadian privacy rights. We deserve, and require, answers on the scope of CSEC's spying programs. We have to ask essential questions: How far have our security agencies gone in the name of security and public safety? What are they capable of? Are any of these invasive spying techniques being used to spy on Canadians at home or abroad? How often is CSEC collecting personal information such as metadata, and which law enforcement and intelligence agencies are they sharing it with?

The Snowden revelations have inspired rigorous debate in the U.S. Congress, statements from the White House, and several lawsuits in the courts. In addition, they have pushed some of the world's largest technology companies to band

together to call for change. The level of response in Canada, however, has been gravely disappointing. Despite almost every major Canadian newspaper conveying in their editorial sections the need for greater transparency and increased oversight, we have had little response or answers from our current government or CSEC itself. This is clearly unacceptable!

In free and open societies, governments must be accessible and transparent to their citizens. Hiding from public scrutiny in the name of security is not only wrong, it is the lazy way out. The federal government must be reminded that it is there at the pleasure of the governed – citizens are entitled to be well-informed about their activities. On the flip side, governments should not have automatic access to information about their citizens. Governments are only permitted to access personal information when authorized by law, and these laws must be clear and protective of privacy. When it comes to the state's power to conduct surveillance, critical privacy protections must include independent court supervision of intrusive powers. Right now, the only form of public accountability and transparency for CSEC rests on an obtuse, after-the-fact, single annual review, undertaken by a single individual with a small staff. This is woefully inadequate for programs which may affect the personal freedoms of all Canadians. At a minimum, what is required is a new legislative mandate to establish a clear structure of accountability.

Snowden's sacrifices have revealed that we all face significant risks associated with unchecked state power. I ask every Canadian to keep the pressure on our leaders for some answers. We must explore new ways forward and create a more open dialogue with the public to ensure that both privacy and civil liberties are preserved. We must continue to pursue all means in order to engage citizens and elected officials. The message of "respect our privacy, respect our freedoms," must be heard, loud and clear. In a free and open society, we deserve no less.

De-identification: A Strong Tool for Protecting Privacy

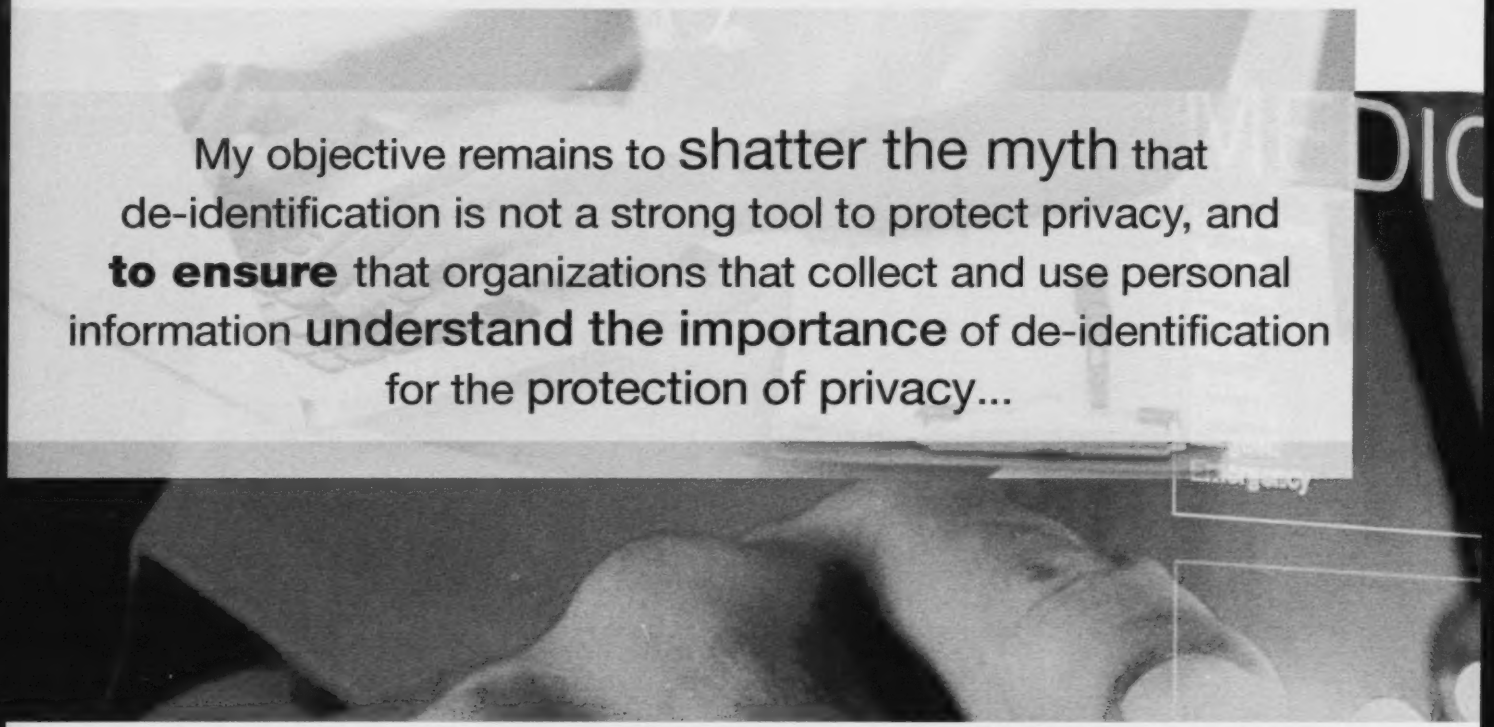
In 2013, I continued my campaign of promoting the de-identification of data as a crucial tool in the protection of privacy, and dispelling the myths about re-identification – by launching the *Privacy by Design De-identification Centre.*

De-identification is a valuable tool that drastically reduces the risk that personal information will be used or disclosed for unauthorized or malicious purposes, while enabling the information to be used for authorized secondary purposes, resulting in benefits to both individuals and society as a whole. It can be done in a way that minimizes the risk of re-identification while also maintaining a high level of data quality. This enables a shift from a zero-sum to a positive-sum paradigm, a win-win solution that is a key principle of *Privacy by Design.*

For example, de-identification is particularly valuable in the context of personal health information, which is extremely sensitive and contains some of the most intimate details of one's life. Personal health information requires the strongest privacy and security protections to prevent unauthorized collection, use and disclosure. However, under appropriate circumstances, it is also important to provide access to health information for secondary purposes that are strongly in the public interest, such as cancer research.

Dispelling the Myths

Contrary to what has been suggested by some critics, re-identification of properly de-identified information is not in fact an "easy" or "trivial" task. It requires concerted effort, on the part of skilled technicians. I made this point more than clear in a paper I published with Professor Khaled El Emam entitled, *Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy,* which was a response to a growing number of claims regarding the ease of re-identification. In


My objective remains to shatter the myth that de-identification is not a strong tool to protect privacy, and **to ensure** that organizations that collect and use personal information **understand the importance** of de-identification for the protection of privacy...

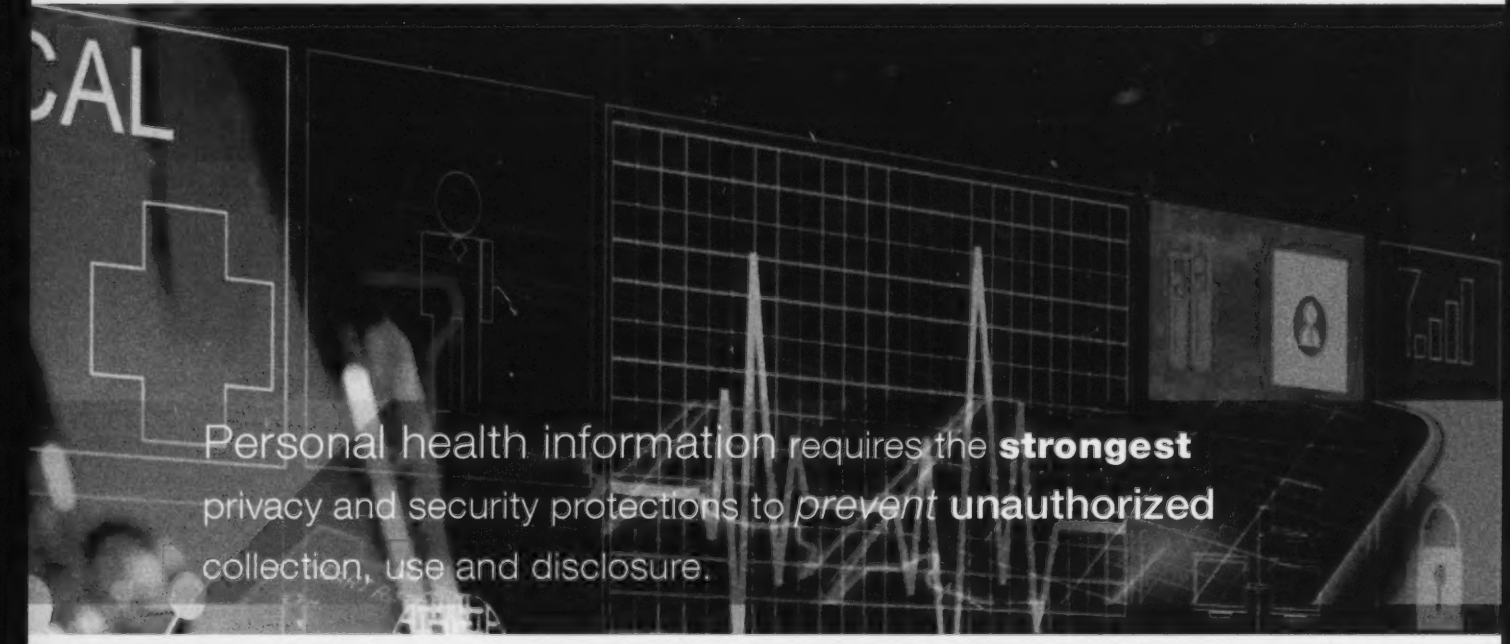
fact, this paper introduced a tool that minimizes the risk of re-identification, while maintaining a high level of data quality.

My objective remains to shatter the myth that de-identification is not a strong tool to protect privacy, and to ensure that organizations that collect and use personal information understand the importance of de-identification for the protection of privacy, and continue to use this tool to the greatest extent possible to minimize potential risks. While my primary focus is on the value of de-identification in the context of personal health information, the same arguments apply in the broader context of personal information being used by governments, business, and other organizations.

However, as re-identification techniques become more sophisticated and more personal information becomes available to facilitate re-identification, it is important to reassess and strengthen de-identification and re-identification risk management techniques. In the vast majority of cases, de-identification will protect the privacy of individuals, as long as the appropriate safeguards are in place. While de-identification may not be a perfect solution to reduce all privacy risks when personal information is being considered for secondary purposes, it is an important first step that should be used as part of an overall risk assessment framework.

Privacy by Design De-identification Centre

To promote the concept of de-identification and to foster proper techniques and best practices, I launched the *Privacy by Design De-identification Centre* in the summer of 2013. I wanted to demonstrate the necessity of de-identification and spread the word on the vital importance of de-identification as a key enabler in protecting privacy. Further, I wanted to create a central place where ideas and research could be explored collaboratively so that we, in the privacy community, could stay ahead of the curve and to be aware and informed of the most up-to-date de-identification techniques and re-identification risk management procedures. I also wanted to promote and foster innovation and promote knowledge-sharing in order to ensure that our privacy remains well protected – now, and well into the future. I maintain an open invitation for anyone to actively participate in the *PbD De-identification Centre*. If you have an idea or question, you can submit a 350 – 500 word blog post to **pbd@ipc.on.ca** to spark a conversation or address a specific issue.


Personal health information requires the **strongest** privacy and security protections to *prevent* **unauthorized** collection, use and disclosure.

Without a written record of how key government decisions are made, transparency is undermined and the basis for policy choices may be shielded from public scrutiny.

ACCESS TO INFORMATION

The movement fosters more transparency and accountability in government and creates more opportunities for meaningful citizen engagement.

Realizing the Economic and Social Benefits of Open Data

The global movement towards Open Data makes vast amounts of machine-readable data freely available to the public. It is one of the truest embodiments of the principles of *Access by Design*, which encourages public institutions to proactively release information as part of an automatic process, rather than waiting for a freedom of information request. The movement fosters more transparency and accountability in government and creates more opportunities for meaningful citizen engagement.

This past September, to mark Right to Know Week 2013, I hosted an event at the Toronto Region Board of Trade, highlighting the accomplishments of the Open Data movement. Its purpose was to demonstrate the enormous economic impact of open government and illustrate how governments and other organizations can benefit when information is automatically pushed out to the public. Speakers highlighted how Open Data has been operationalized by governments and innovators to improve communities. These programs have created engagement, provided businesses with valuable insights, and served as a catalyst for innovation by inspiring the development of new products and services.

Ron McKerlie, Deputy Minister, Open Government for the Ministry of Government Services (pictured above), shared Ontario's vision for open information, data and public dialogue. Over the next few years, the government is striving to: increase public engagement by introducing new tools for consultation; deliver more responsive policies, programs and services; provide more efficient access to government services, data and information; and support economic growth by ensuring data and information is available, accessible and useable. I applaud the government for embracing open government and challenge them to ensure Ontario is a leader, not a follower.

The City of Toronto's Nancy Isozaki highlighted the numerous ways the city has become a Canadian leader in pushing out information. One key example of this leadership is the city's posting all council agendas and reports online, simultaneously allowing citizens to track the status of issues, view council vot-

Ron McKerlie, Deputy Minister, Open Government for the Ministry of Government Services

Nancy Isozaki, Director, Corporate Information Policy, City of Toronto

Stéphane Guidoin, Transportation Director, Open North

ing records, and register to speak about an agenda item.

Rob Giggey demonstrated how the App4Ottawa contests, promoted by the City of Ottawa, have led to the creation of 39 active apps for the public using the city's Open Data sets. Winning entries have included an app which helps select the best recreational activities and an app which monitors the activities of lobbyists.

MaRS Discovery District's Joe Greenwood illustrated how Open Data can create efficiencies and save money in the fields of health care, transportation, and energy. Of particular interest was Ontario's Green Button program, which now has 20 companies building energy monitoring solutions for consumers based on anonymized data from 2.7 million homes and businesses.

The Executive Director of the Open Data Institute of Canada, Dennis Brink, examined the success of Propertize.ca, a website which allows the public to compare area property tax assessments from open information.

Open North's Stéphane Guidoin explored the enormous societal value of Open Data programs. His organization has assisted in implementing *Citizen Budget*, an interactive budget simulator that involves residents in the budget-making process, in various municipal websites across North America.

It was encouraging to see the continued growth of the Open Data movement and so many organizations embracing my concept of *Access by Design*. I will continue to encourage public institutions to become more transparent and push out as much information to the public as possible.

Highlights from 2013 Orders

Municipal

MO-2848
City of Toronto

Two media requesters sought access to the city hall parking pass log sheets for the mayor of Toronto. The city denied access, claiming that disclosure would be an unjustified invasion of privacy, compromise law enforcement interests, and threaten health and safety. In this order, the adjudicator found that the record is not exempt and ordered it to be disclosed to the appellants. Among other things, the adjudicator determined that the information in the log sheets is not personal information.

MO-2964-I
City of Greater Sudbury

The City received six requests for the "current and any previous" employment contracts of six named city employees. While the city's decision raised a number of issues, this interim order addressed access issues in which the city claimed the records were exempt from disclosure because they would reveal the substance of deliberations at closed meetings. The adjudicator found that these employment contracts do not qualify for exemption. While the executed contracts represent the *product* of in-camera discussions, they do not reveal the *substance* of the deliberations at the closed meetings. The adjudicator also determined that the portions of these records that describe employment benefits must be disclosed. Decisions regarding access to the remaining portions of the records are reserved.

Provincial

PO-3233
Carleton University

A media outlet requested access to specific student grade information from 1999 to 2011. The university denied access to the information, claiming that its disclosure would result in an unjustified invasion of students' personal privacy and prejudice the university's economic

Access by Design and Open Data Movement, Bringing Tangible Social and Economic Value – Dr. Ann Cavoukian, Information and Privacy Commissioner, Ontario; Ron McKerlie, Deputy Minister, Open Government , Ministry of Government Services; Nancy Isozaki, Director, Corporate Information Policy, Corporate Information Management Services, City of Toronto; Rob Giggey, Strategic Support Coordinator & Open Data Lead, City of Ottawa; Stéphane Guidoin, Transportation Director, Open North; Joe Greenwood, Program Director, MaRS Discovery District; Dennis Brink, Executive Director, Open Data Institute of Canada

interests or competitive position. In this order, the adjudicator found that the responsive grade information, which is anonymized, does not fit within the definition of personal information in the *Freedom of Information and Protection of Privacy Act*, as it does not relate to identifiable individuals. The personal privacy exemption therefore cannot apply. The adjudicator also rejected the university's claim that disclosure would prejudice its competitive and economic interests. As no exemptions apply to the grade data, the university was ordered to disclose the requested information.

PO-3240
Ministry of Natural Resources

A freedom of information request was made for information relating to an Adaptive Management Plan submitted by a company in support of a licence application to expand a quarry. The ministry located an email responsive to the request, authored by a ministry biologist regarding environmental mitigation strategies described in the Adaptive Management Plan. It denied access to the email, in its entirety, relying on the exemption under the *Freedom of Information and Protection of Privacy Act*, for information that would reveal advice or recommendations. The requester appealed the decision, taking the position that this exemption did not apply and, if it did, the public interest override provision in the *Act* should permit disclosure. The adjudicator found that the information at issue consists of advice or recommendations that are exempt from disclosure, but a compelling public interest in the disclosure of that information overrides the purpose of the exemption. The adjudicator ordered disclosure of the email.

Stop Using Privacy as a Shield

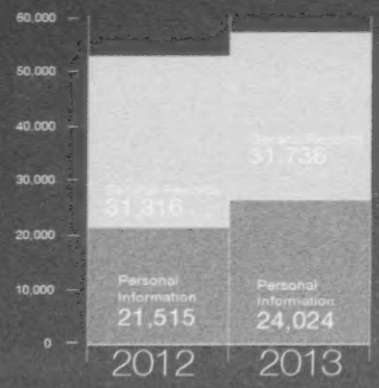
On occasion, privacy and privacy laws are cited by public institutions as the reason for not releasing general records that have been requested by the public or the media. This is unfortunate, as these laws are designed to protect personal privacy, not prevent the sharing of information. Privacy is the fundamental right that helps us to realize the other rights that we value so dearly, such as liberty and freedom. To cite this right as a barrier to releasing data which does not contain personal information devalues the meaning of privacy and damages the public's trust.

In my experience, the reasoning behind this excuse is an effort to play it safe, instead of gaining a proper understanding of what the options are for disclosure, or in the worst cases, using it as a convenient diversion for inaction. The latter is usually an attempt to withhold information that potentially might be harshly scrutinized by the public or the media.

Discretion should always be exercised before disclosing information, but privacy must not be used as a shield. Government organizations need to strive towards creating methods of pushing out information to ensure greater transparency and a culture of accountability – a win-win situation for everyone involved.

As I look back on the past years of the IPC, I feel that Ontarians can be assured that this office has grown into a first-class agency, known around the world for demonstrating innovation and leadership, in the fields of both access and privacy.

STATISTICS



OVERALL REQUESTS

↑12% Personal Information

↑1% General Records

↑6% Total Requests

2013 AT A GLANCE

PROVINCIAL SUMMARY

PERSONAL INFORMATION

REQUESTS
2013 6,825 ↑17%
2012 5,813

APPEALS OPENED
2013 186 ↑14%
2012 163

APPEALS CLOSED
2013 143 ↓13%
2012 164

AVERAGE COST
2013 $6.04 ↑21%
2012 $4.98

GENERAL RECORDS

REQUESTS
2013 13,996 ↓1%
2012 14,158

APPEALS OPENED
2013 421 ↓8%
2012 456

APPEALS CLOSED
2013 454 ↑15%
2012 395

AVERAGE COST
2013 $40.57 ↓3%
2012 $41.99

TOTAL REQUESTS
2013 20,821 ↑4%
2012 19,971

PRIVACY COMPLAINTS OPENED
2013 120 ↓23%
2012 155

PRIVACY COMPLAINTS CLOSED
2013 118 ↑23%
2012 154

MUNICIPAL SUMMARY

PERSONAL INFORMATION

REQUESTS
2013 16,726 ↑7%
2012 15,702

APPEALS OPENED
2013 245 ↓8%
2012 265

APPEALS CLOSED
2013 255 ↑11%
2012 230

AVERAGE COST
2013 $8.24 ↓15%
2012 $9.67

GENERAL RECORDS

REQUESTS
2013 17,304 ↑1%
2012 17,158

APPEALS OPENED
2013 433 ↑10%
2012 392

APPEALS CLOSED
2013 386 ↑5%
2012 369

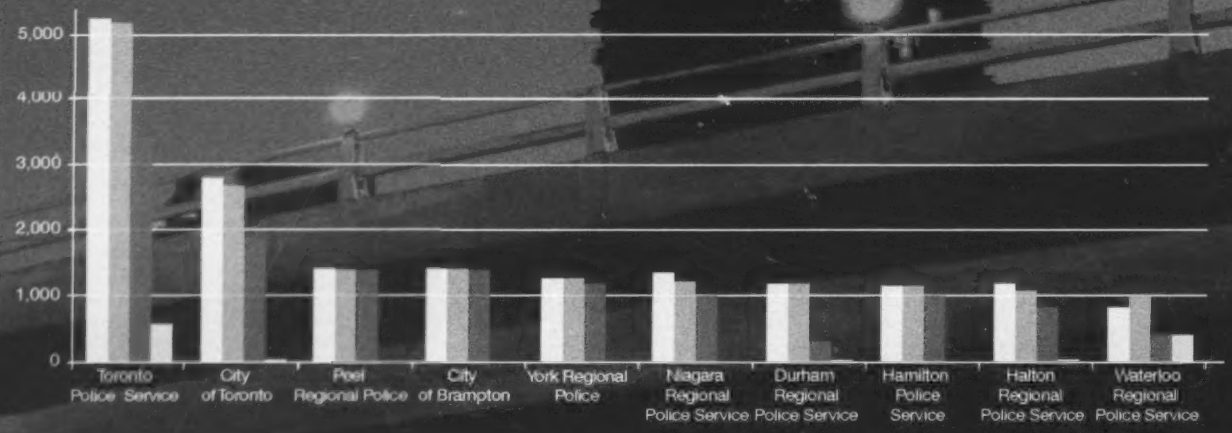
AVERAGE COST
2013 $28.09 ↑3%
2012 $27.30

TOTAL REQUESTS
2013 34,030 ↑4%
2012 32,860

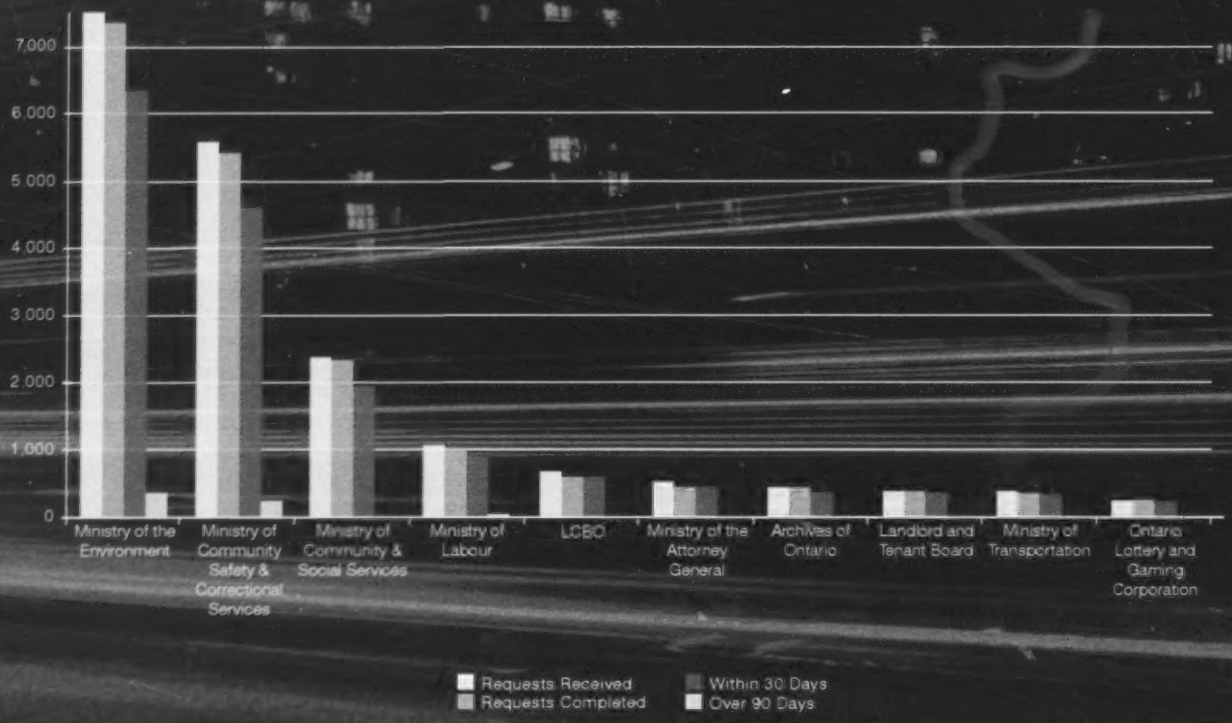
PRIVACY COMPLAINTS OPENED
2013 136 ↑7%
2012 127

PRIVACY COMPLAINTS CLOSED
2013 141 ↑17%
2012 121

TOP 10 MUNICIPAL INSTITUTIONS



TOP 10 PROVINCIAL INSTITUTIONS



Ranked by number of requests completed in 2013.

2013 HIGHLIGHTS

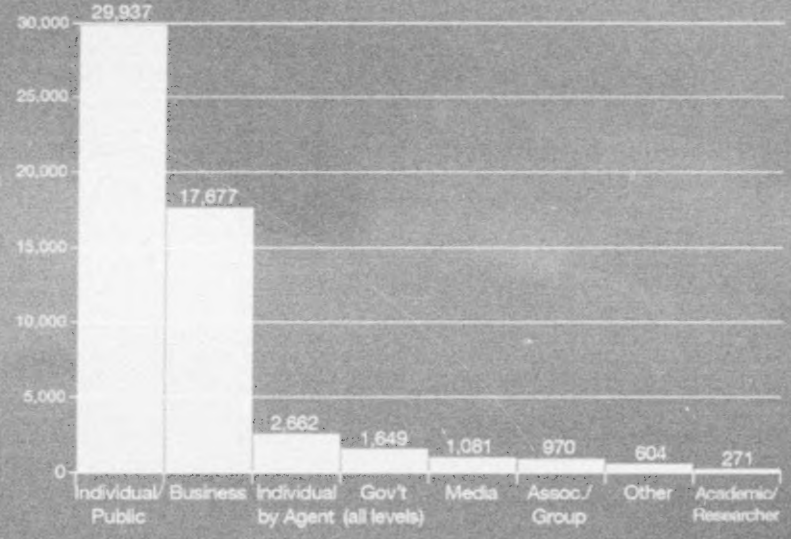
55,760
Freedom of information (FOI) requests filed across Ontario in 2013

34,329
Municipal requests filed

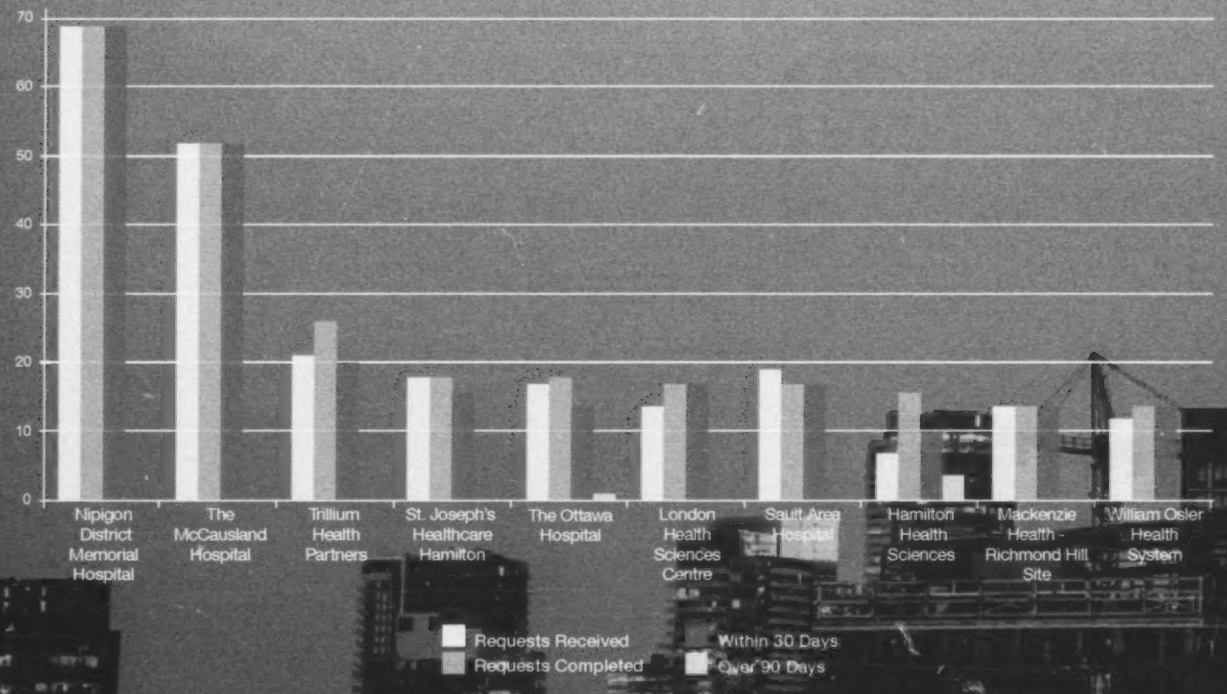
21,431
Provincial requests filed

54,851
FOI requests completed in Ontario in 2013

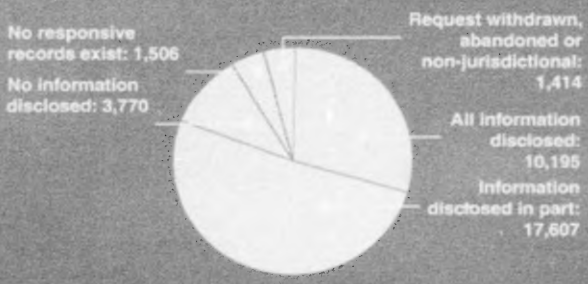
REQUESTS COMPLETED BY SOURCE



TOP 10 HOSPITALS

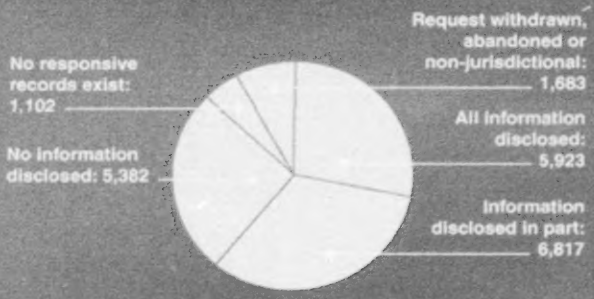


OUTCOME OF REQUESTS: MUNICIPAL


No responsive records exist: 1,506
No information disclosed: 3,770
Request withdrawn, abandoned or non-jurisdictional: 1,414
All information disclosed: 10,195
Information disclosed in part: 17,607

* Totals do not balance back to total requests completed because the counts in this table also include requests where no decision was issued due to the request being outside the institution's jurisdiction

OUTCOME OF REQUESTS: PROVINCIAL


No responsive records exist: 1,102
No information disclosed: 5,382
Request withdrawn, abandoned or non-jurisdictional: 1,683
All information disclosed: 5,923
Information disclosed in part: 6,817

* Totals do not balance back to total requests completed because the counts in this table also include requests where no decision was issued due to the request being outside the institution's jurisdiction

$8.24 Personal Information

$28.09 General Records

Average Cost of Municipal Requests

$6.04 Personal Information

$40.57 General Records

Average Cost of Provincial Requests

16,118

Requests where all information was disclosed

86.5%

30-day compliance rate for provincial ministries, agencies and institutions

77.2%

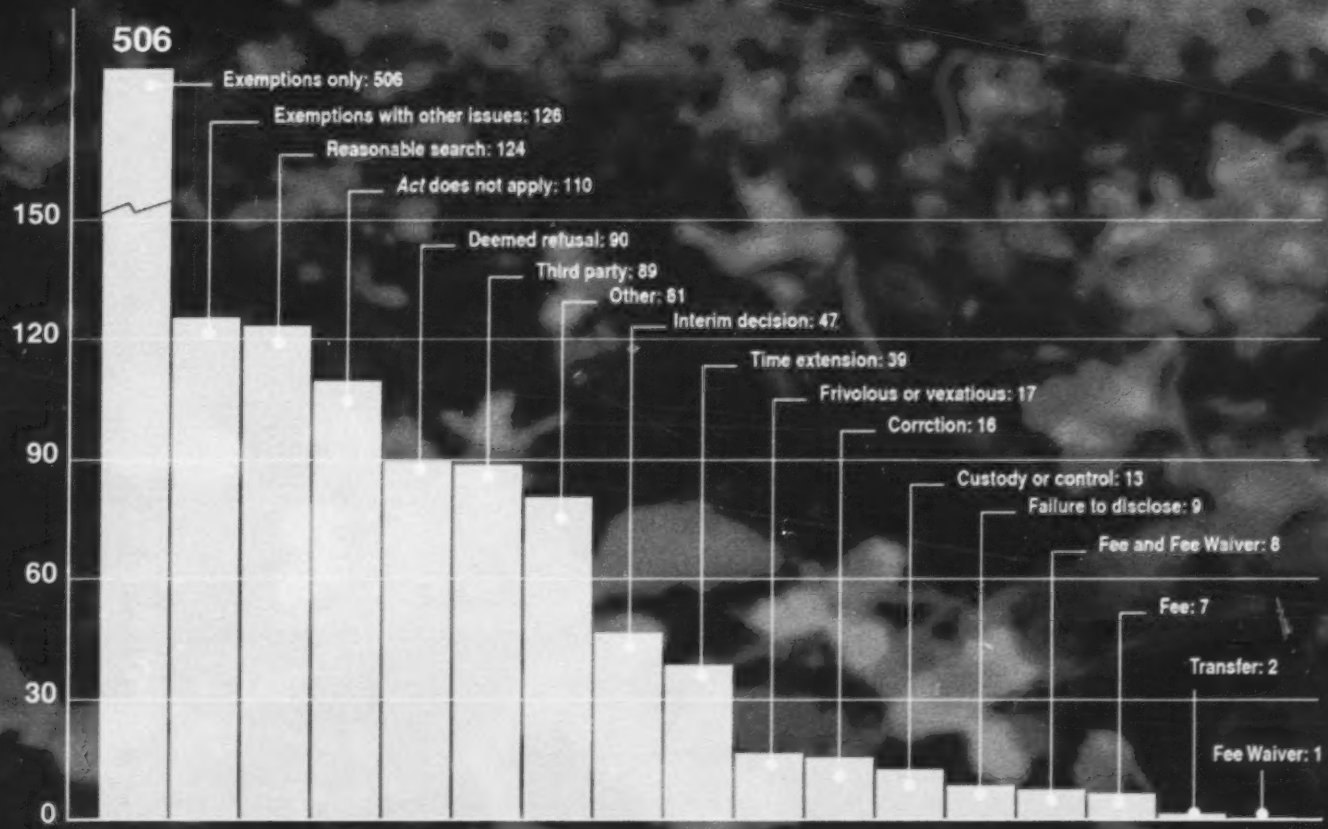
30-day compliance rate for municipal government organizations

1,285
Appeals opened by the IPC in 2013

53.3%
Appeals were mediated in full

11.7%
Appeals were withdrawn

ISSUES IN APPEALS OPENED



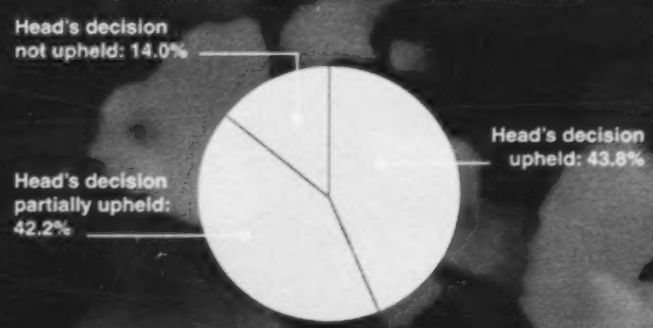
322
Appeals resulted in an Order

481
Appeals were closed at the mediation stage

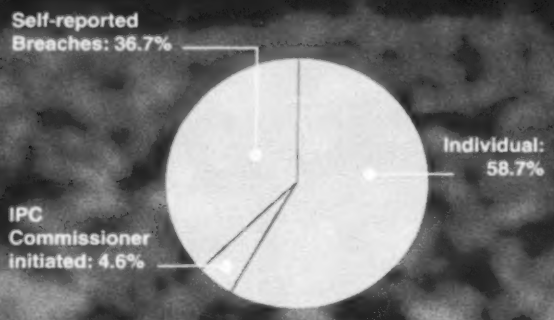
1,002
Appellants were individual citizens

173
Appellants were businesses

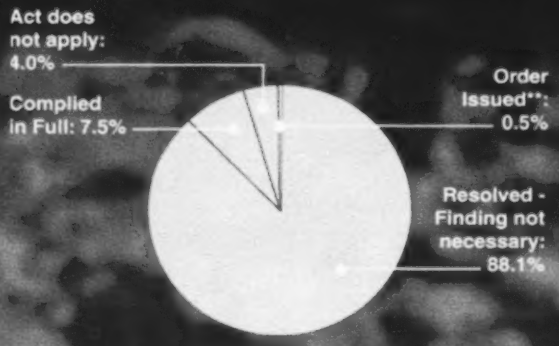
NUMBER OF APPEALS CLOSED BY ORDER



SOURCE OF COMPLAINTS



OUTCOME OF ISSUES* IN PRIVACY COMPLAINTS



* The number of issues does not equal the number of complaints closed, as some complaints may involve more than one issue. Abandoned, withdrawn and screened out complaint files are not included.

** Privacy Complaint File PC12-47 closed by order PO-3171

256
Privacy complaints opened in 2013

259
Privacy complaints closed in 2013

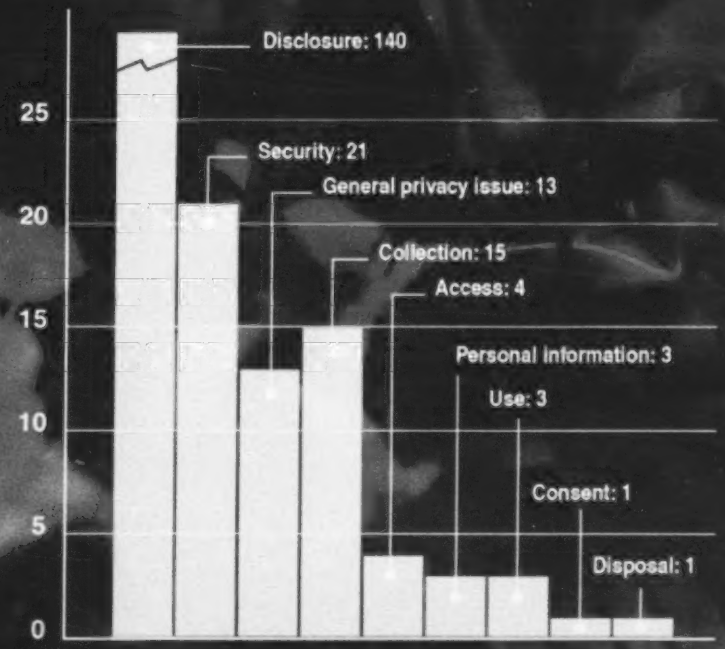
66%
Privacy complaints resolved

14.3%
Privacy complaints withdrawn

152
Privacy complaints filed by individuals

95
Privacy complaints were self-reported breaches

ISSUES* IN PRIVACY COMPLAINTS



* The number of issues does not equal the number of complaints closed, as some complaints may involve more than one issue. Abandoned, withdrawn and screened out complaint files are not included.

Judicial Reviews

***Ministry of Community and Social Services v. Information and Privacy Commissioner et al.*, 2014 ONSC 239 – Judicial Review of Order PO-2917**

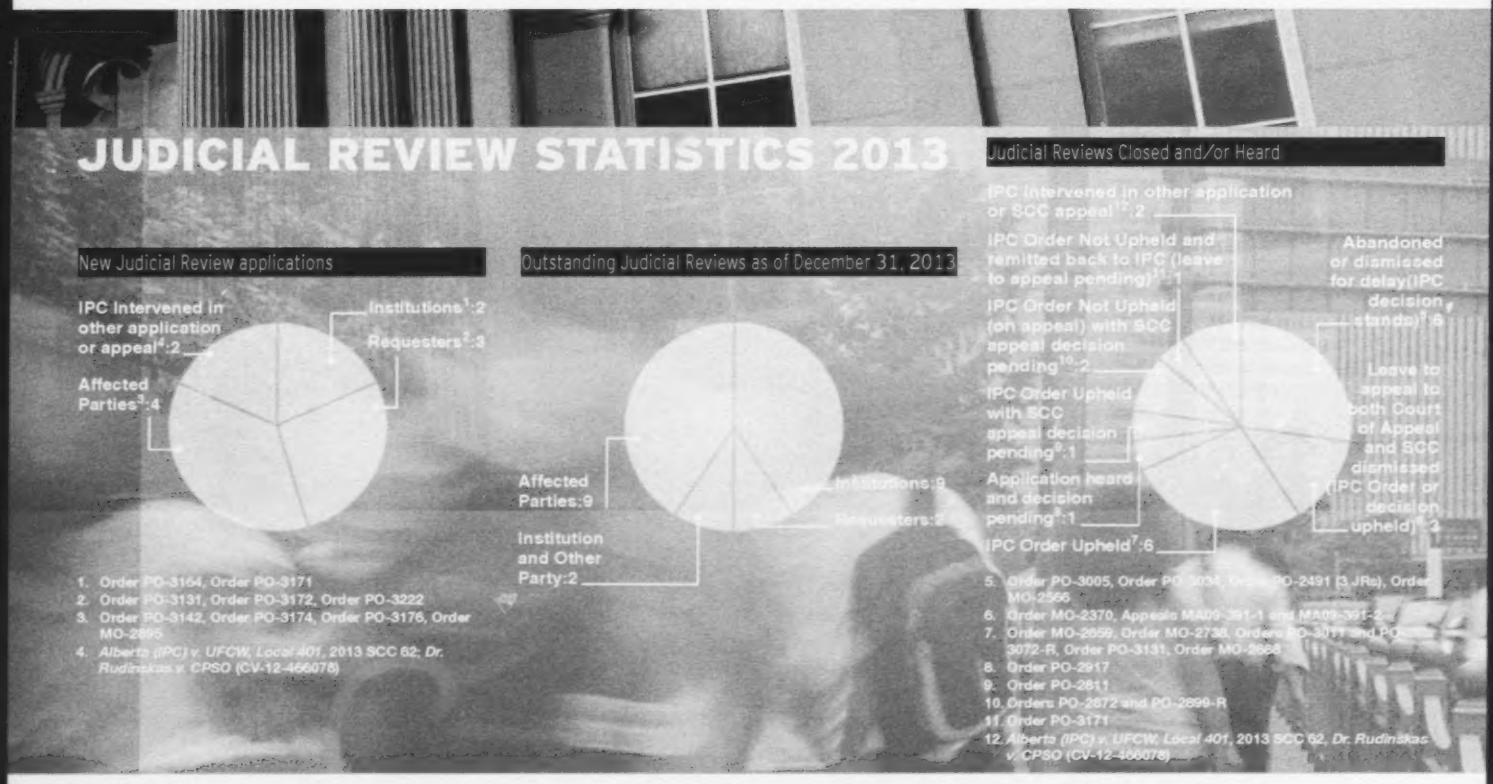
In an important decision released early this year, the Ontario Divisional Court dismissed an application for judicial review brought by the Ministry of Community and Social Services challenging the IPC's order to disclose the requester's personal information, including the full names of Family Responsibility Office (FRO) employees who worked on his file.

In the IPC's inquiry, the Ministry and the Ontario Public Service Employees Union (OPSEU) claimed that the full names of FRO employees on records contained in the requester's file were excluded from *Freedom of Information and Protection of Privacy Act* (*FIPPA*) by the labour relations exclusion at s. 65(6)3. Alternatively, the names were subject to the exemptions at ss. 14(1)(e) and 20 for threats to health and safety. Because FRO employees had received threats over the years from support payors, OPSEU had filed a grievance claiming that disclosure of the full names would jeopardize the health and safety of employees and their families by exposing their identities to disgruntled FRO payors who might act on their threats. The grievance was resolved by a settlement agreement which permitted (but did not require) FRO staff to withhold their full names from the public in written and telephone communications and to use, instead, their first names and an identifying number. The settlement was then incorporated into a "consent order" issued by the Grievance Settlement Board (GSB).

The Ministry and OPSEU argued that the exclusion applied because, as a result of the GSB consent order, the full names relate to communications "about labour relations or employment related matters" within the meaning of s. 65(6)3. Even if not excluded, disclosure of the names would threaten the health and safety of employees within the meaning of the ss. 14(1)(e) and 20. In addition, disclosure under *FIPPA* would be in conflict with the consent order.

The IPC rejected all of these arguments. The adjudicator found that records containing the names of employees were not "about" labour relations, but were routine operational records about the core business of FRO. The IPC also rejected the application of ss. 14(1)(e) and 20 because: (1) there was no evidence that the requester posed a threat to any FRO employees; (2) there was no evidence that the employees in question had ever been subject to any threats; and (3) the information in the records was not potentially inflammatory.

In dismissing the Ministry's application for judicial review, the Divisional Court made several important rul


JUDICIAL REVIEW STATISTICS 2013
New Judicial Review applications
IPC Intervened in other application or appeal[4]:2
Institutions[1]:2
Requesters[2]:3
Affected Parties[3]:4
1. Order PO-3164, Order PO-3171
2. Order PO-3131, Order PO-3172, Order PO-3222
3. Order PO-3142, Order PO-3174, Order PO-3176, Order MO-2895
4. Alberta (IPC) v. UFCW, Local 401, 2013 SCC 62; Dr. Rudinskas v. CPSO (CV-12-466078)
Outstanding Judicial Reviews as of December 31, 2013
Affected Parties:9
Institution and Other Party:2
Institutions:9
Requesters:2
Judicial Reviews Closed and/or Heard
IPC Intervened in other application or SCC appeal[12]:2
IPC Order Not Upheld and remitted back to IPC (leave to appeal pending)[11]:1
IPC Order Not Upheld (on appeal) with SCC appeal decision pending[10]:2
IPC Order Upheld with SCC appeal decision pending[9]:1
Application heard and decision pending[8]:1
IPC Order Upheld[7]:6
Abandoned or dismissed for delay(IPC decision stands)[6]:6
Leave to appeal to both Court of Appeal and SCC dismissed (IPC Order or decision upheld)[5]:2
5. Order PO-3005, Order PO-3034, Order PO-2491 (3 JRs), Order MO-2566
6. Order MO-2370, Appeals MA09-391-1 and MA09-391-2
7. Order MO-2659, Order MO-2730, Orders PO-3011 and PO-3072-R, Order PO-3131, Order MO-2866
8. Order PO-2917
9. Order PO-2811
10. Orders PO-2672 and PO-2899-R
11. Order PO-3171
12. Alberta (IPC) v. UFCW, Local 401, 2013 SCC 62, Dr. Rudinskas v. CPSO (CV-12-466078)

ings with broad implications for the operation of *FIPPA* in the future.

First, applying recent judgments of the Supreme Court of Canada, the Court refused to follow earlier rulings and held that the standard of review for IPC decisions applying the exclusion at s. 65(6) is reasonableness, not correctness.

Second, the Court rejected the Ministry's broad interpretation of s. 65(6) which could potentially exclude routine operational records from *FIPPA* and "subvert the principle of openness and public accountability that the *Act* is designed to foster."

Third, in rejecting the Ministry's threat to safety arguments, the Court made several observations about the operation of the *Act* which the IPC has been urging on it for years:

1. A requester's reason for requesting or a demonstrated "need" for the information is irrelevant.
2. The individual's right of access to his or her own personal information under Part III of *FIPPA* is to be assessed differently from general right of access at Part II: "A requester under s. 47(1)(b) starts with the presumption that he or she is entitled to the information."
3. Disclosure of records under Part II of the *Act* is "disclosure to the world"; disclosure of personal information under Part III is to the requesting individual only.
4. Evidence of a general risk of harm from disclosure to the public is not necessarily sufficient to show harm when disclosing a requester's personal information.
5. The Minister's discretion to disclose a record subject to a discretionary exemption (in this case ss. 14(1(e) and 20) cannot be fettered by an agreement such as the GSB consent order: "The Minister cannot consent to an arrangement that would have the effect of contracting out of his or her obligations under the *Act*."

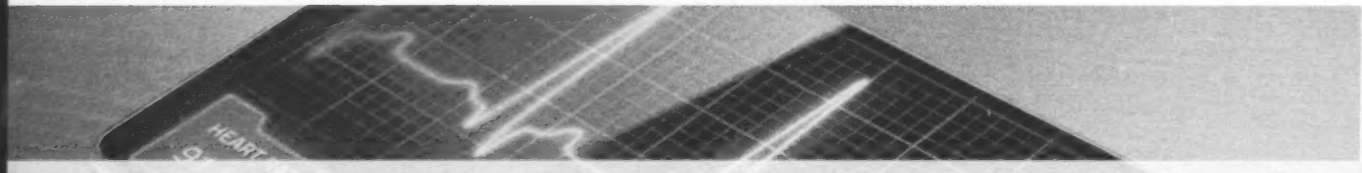
Finally, the Court affirmed the principle that it will not actively seek out "operational conflict" between the decisions of two administrative tribunals. The Court observed that the order for disclosure did not affect the ability of FRO employees to choose not to use their full names in their dealings with the public. Accordingly, the GSB order did not conflict with or take precedence over the IPC's decision.

Personal Health Information Protection Act in 2013

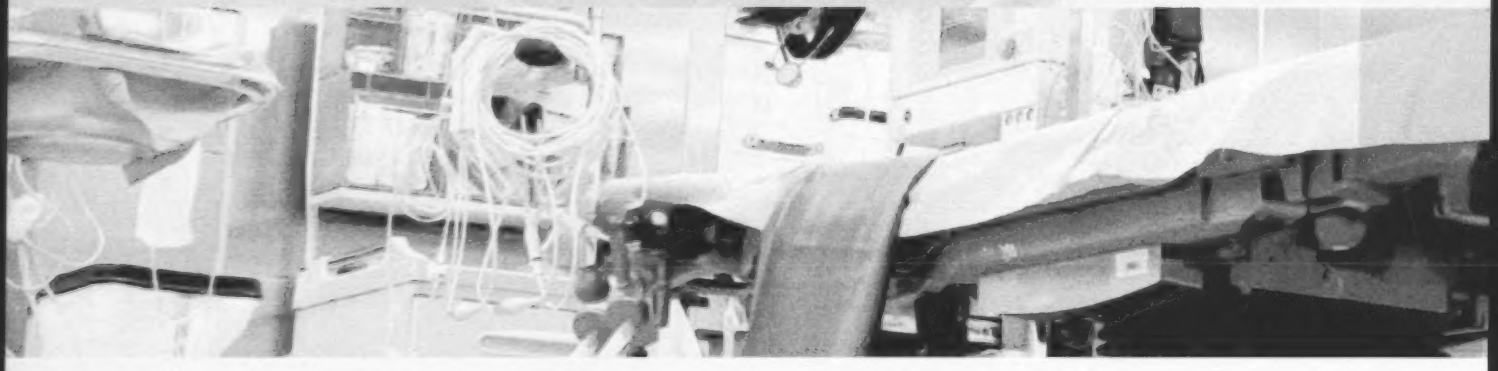
As with all years past, this year was a busy one regarding the *Personal Health Information Protection Act* (*PHIPA*), with both challenges and advancements. While the government moved forward on Bill 78, The *Electronic Personal Health Information Protection Act*, we experienced more *PHIPA* breaches of personal health information, which further gave relevance to our work on the growing practice of Bring Your Own Device (BYOD).

Bill 78, *Electronic Personal Health Information Protection Act*

In May, the government of Ontario introduced amendments to *PHIPA* – which I had been advocating for some time – addressing the privacy and security issues associated with electronic health records. While *PHIPA* has served as a model for health privacy legislation across Canada since it was introduced in 2004, it did not adequately address the rights of individuals and the duties of health-care providers in a shared electronic health record environment. The proposed amendments to *PHIPA* will clarify the right of patients to limit the collection, use and disclosure of their personal health information (PHI) in the electronic health record for health-care purposes through the application of consent directives. The proposed amendments will also clarify the right of patients to access, request a correction, and find out who has accessed their electronic health records. Further,



The proposed amendment to *PHIPA* will facilitate the introduction of electronic health records and, in turn, **modernize the delivery of health care** throughout Ontario.



the proposed amendments will also assure patients that only their authorized health-care providers, and those acting on their behalf, will be able to directly access the PHI in their electronic health record, and will limit the purposes for which such information may be accessed. There will also be a requirement to log and monitor all accesses to electronic health records to prevent any unauthorized collection, use, and disclosure of personal health information.

The proposed amendments to *PHIPA* will facilitate the introduction of electronic health records and, in turn, modernize the delivery of health care throughout Ontario. Such records have the potential to greatly improve diagnosis and treatment; to enhance patient safety; and to facilitate the coordination and integration of services – resulting in a more efficient and effective health system.

Bring Your Own Device

Lost and stolen mobile computing and storage devices (laptops, tablets, smartphones, USB drives and memory cards) are the single biggest cause of security and privacy breaches today — and also one of the most foreseeable and preventable of risks.

While I was hoping, as always, to have a year free of reported privacy breaches, 2013 proved to be no exception. This year there were a number of breaches involving PHI, almost all of which involved mobile devices. For example, the theft of a memory card containing the unencrypted PHI of more than 18,000 Peel Region Public Health patients illustrates just how vulnerable privacy is becoming in an environment increasingly dependent on mobile computing devices.

While the headline message arising from my office's breach investigations is that health-care custodians must deploy strong encryption and password protection on all mobile devices, in practice there are rarely simple technical fixes to prevent "data leakage" in complex, high-availability environments. Effective life cycle management of data requires a structured and standards-based approach to information risk management and should be composed of a core set of IT governance objectives addressing data loss prevention, as we advocated in our December 2012 joint paper, *Encryption by Default and Circles of Trust: Strategies to Secure Per-*

sonal Information in High-Availability Environments, with Sunnybrook Health Sciences Centre and CryptoMill Technologies Ltd.

The need to adopt a comprehensive and systematic approach to mobile device management security is a major message of my joint paper with Telus concerning the growing practice known as *Bring Your Own Device* (BYOD), where organizations allow employees to use their personal devices for work-related purposes. Canadian firms now lead the world in adopting the bring-your-own-device trend and deploying consumer-type applications in the workplace. At the same time, however, more than half of Canadian organizations are losing sensitive data through employee operated devices each year.

The purpose of this joint paper, entitled, *BYOD: (Bring Your Own Device) Is Your Organization Ready?* is to provide practical information on how to identify and address the different privacy concerns raised by a BYOD program. This can be accomplished by following five key steps, from requirements documentation to end-user support, as outlined in the paper. When applied, these steps express foundational *PbD Principles* such as proactivity, embedded methods, positive-sum results, and end-to-end safeguards with no loss of functionality.

This guidance is as timely today. More and more health care organizations are facing growing pressures to allow employees, and physicians who are not employees of hospitals, to connect their personal mobile devices to corporate networks. However, the blurring of personal and business use of a mobile device raises many privacy and security concerns, which, if not properly addressed, may result in privacy breaches, effectively turning the benefits of BYOD into losses to the organization.

BYOD is now an unstoppable trend, offering new benefits and risks – notably data security risks – to organizations of all sizes. Fortunately, I feel that it is now possible to manage both benefits and risks in an optimal way by adopting a comprehensive *Privacy by Design* approach.

To provide additional guidance for health-care organizations and other institutions on how to identify and address general privacy concerns related to the use of mobile devices in the workplace, I released a companion brochure, *Safeguarding Privacy on Mobile Devices.* It offers practical tips for protecting PHI and personally identifiable information when using a mobile device.

Financial Statement

	2013-2014 Estimates $	2013-2013 Estimates $	2012-2013 Actual $
SALARIES AND WAGES	10,211,500	10,132,000	9,663,655
EMPLOYEE BENEFITS	2,348,900	2,330,900	1,847,769
TRANSPORTATION AND COMMUNICATIONS	337,500	337,500	231,119
SERVICES	1,960,300	1,960,300	1,785,107
SUPPLIES AND EQUIPMENT	336,000	336,000	319,067
TOTAL	15,194,200	15,096,700	13,846,717

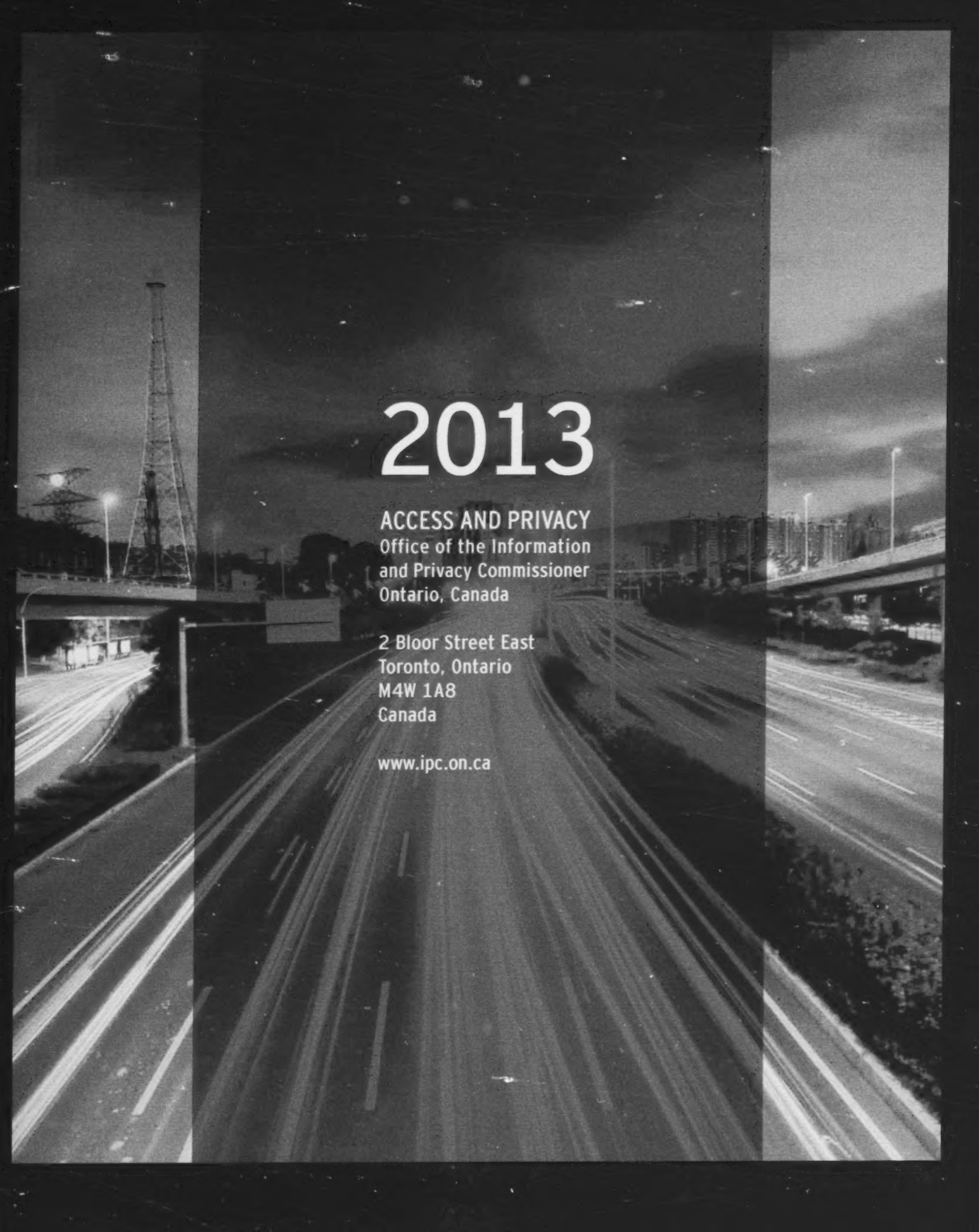
Note: The IPC's fiscal year begins April 1 and ends March 31.
The financial statement of the IPC is audited on an annual basis by the Office of the Auditor General of Ontario.

2013 APPEALS FEES DEPOSIT

(Calendar year)

GENERAL INFO.	PERSONAL INFO.	TOTAL
$15,039	$2,940	$17,979

See further financial information, including IPC Public Sector Salary Disclosure, at ***www.ipc.on.ca***



2013

ACCESS AND PRIVACY

Office of the Information
and Privacy Commissioner
Ontario, Canada

2 Bloor Street East
Toronto, Ontario
M4W 1A8
Canada

www.ipc.on.ca